МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра інформаційних технологій та комп’ютерної інженерії

А.Ю. Дереза, Я.І. Шедловська, І.А. Шедловський

ЗАХИСТ ІНФОРМАЦІЇ В КОМП’ЮТЕРНИХ СИСТЕМАХ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня магістра
галузі знань F Інформаційні технології

Дніпро
НТУ «ДП»
2025

Дереза А.Ю.

Захист інформації в комп'ютерних системах [Електронний ресурс] : методичні рекомендації до виконання лабораторних робіт для здобувачів ступеня магістра галузі знань F Інформаційні технології / А.Ю. Дереза, Я.І. Шедловська, І.А. Шедловський ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2025. – 56 с.

Автори:
А.Ю. Дереза, канд. техн. наук, доц.
І.А. Шедловський, канд. техн. наук, доц.
Я.І. Шедловська, канд. техн. наук, доц.

Затверджено науково-методичною комісією зі спеціальності 123 Комп’ютерна інженерія (протокол № 4 від 14.04.2025 р.) за поданням кафедри інформаційних технологій та комп’ютерної інженерії (протокол № 13 від 11.04.2025 р.).

Уміщено теоретичні відомості за темами лекційного курсу, варіанти лабораторних завдань з рекомендаціями до їх виконання, контрольні питання, список використаної та рекомендованої літератури.

Зміст методичних рекомендацій відповідає програмі вибіркової навчальної дисципліни «Захист інформації в комп'ютерних системах» і адресовано студентам, які проходять підготовку за спеціальностями галузі знань F Інформаційні технології.

Відповідальний за випуск завідувач кафедри інформаційних технологій та комп’ютерної інженерії В. В. Гнатушенко, д-р техн. наук, проф.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Курс «Захист інформації в комп’ютерних системах» готує слухачів до сертифікаційного іспиту Implementing Cisco Network Security (IINS) (210-260), після якого можна отримати сертифікацію CCNA Security.

Інформаційні процеси, що проходять повсюдно у світі, висувають на перший план, поряд із задачами ефективного опрацювання і передачі інформації, найважливішу задачу забезпечення безпеки інформації. Це пояснюється особливою значимістю для розвитку держави його інформаційних ресурсів, зростанням вартості інформації в умовах ринку, її високою уразливістю і нерідко значним збитком у результаті її несанкціонованого використання.

Методичні рекомендації призначені для закріплення теоретичних знань, набутих студентами в лекційному курсі, формування компетентностей щодо методів захисту інформації у комп'ютерних системах. У курсі розглядаються основні підходи до забезпечення інформаційної безпеки комп'ютерних систем, базові технології захисту міжмережевого обміну даними, методи програмного та апаратного захисту.

У підсумку виконання лабораторних робіт студенти – майбутні фахівці повинні отримати результати навчання у відповідності з вимогами освітньої програми, які представлені в табл. 1.1.

Таблиця 1.1 Результати навчання, що отримуються у підсумку виконання лабораторних робіт з дисципліни “Захист інформації в комп’ютерних системах”.

Дисциплінарні результати навчання (ДРН)	
шифр ДРН	**зміст**
ДРН-1	Демонструвати знання складу і принципи функціонування систем захисту інформації, та обґрунтовувати вибір методів захисту інформації у комп'ютерних системах
ДРН-2	Виявляти і усувати потенційно небезпечні місця у системі безпеки; розробляти комплексну політику мережевої безпеки; впроваджувати модель AAA на мережевих пристроях; конфігурувати систему запобігання вторгнень (IPS)
ДРН-3	Знати принципи роботи основних типів шкідливих комп’ютерних програм і застосовувати методи боротьби з ними
ДРН-4	Вміти конфігурувати пристрої локальної мережі для контролю доступу, захисту мережевих пристроїв і систем, а також підтримки цілісності і конфіденційності мережевого трафіку Налаштовувати функціонування міжмережевих екранів на різних рівнях моделі OSI.
ДРН-5	Застосовувати організацію захищеного віддаленого доступу користувачів; налаштовувати статичні (site-to-site) VPN з'єднання.
ДРН-6	Застосовувати симетричні та асиметричні алгоритми шифрування даних.
ДРН-7	Розробляти та використовувати сучасні засоби та методи криптографічного захисту інформації.

Мета лабораторних робіт – поглибити і систематизувати набуті студентами на лекціях теоретичні знання з дисципліни та сформувати у майбутніх фахівців з інформаційних систем та технологій професійних компетентностей (знань, умінь і навичок) використання методів, програмного забезпечення та інформаційних технологій з забезпечення інформаційної безпеки.

Лабораторні роботи передбачають застосування загальновідомих підходів та програмних засобів, які можуть бути використані для аналізу інформаційних потоків та стану кібербезпеки. Кожна лабораторна робота має назву, ціль, постановку задачі, контрольні питання і завдання, рекомендації щодо виконання роботи та вимоги до оформлення звіту, а також варіанти індивідуальних завдань.

Одержання результатів робіт передбачено розрахунковими методами з використанням комп'ютерної техніки, яка працює на платформі Windows та програмного середовища Wireshark, доступ до сервісів за допомогою віртуальних машин Oracle VM VirtualBox та HDP Sandbox.

2. ПОСТАНОВКА ЗАДАЧ ЛАБОРАТОРНИХ РОБІТ, МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДЛЯ ЇХ ВИКОНАННЯ

2.1 Лабораторна робота № 1
Дослідження з кібербезпеки

Об’єкт: високопрофесійні кібератаки.

Мета: аналіз кібератаки.

Стислі теоретичні відомості

Уряди, підприємства та окремі користувачі все частіше стають об'єктами кібератак, і експерти прогнозують, що ці атаки, ймовірно, збільшаться в майбутньому.

Освіта у сфері кібербезпеки є одним з головних міжнародних пріоритетів, оскільки гучні інциденти, пов'язані з кібербезпекою, викликають побоювання, що атаки можуть загрожувати глобальній економіці.

Центр стратегічних та міжнародних досліджень оцінює, що вартість кіберзлочинності для світової економіки становить понад 600 мільярдів доларів щорічно. У цій лабораторній роботі ви будете розглядати чотири високопрофесійні кібератаки і будете підготовленими до обговорення того, хто, що, чому і як щодо кожної атаки.

Потрібно

Частина 1: Проведіть пошук гучних кібератак.

a. Використовуючи улюблену пошукову систему, виконайте пошук кожної з перелічених нижче кібератак. Ваш пошук, ймовірно, призведе до кількох результатів, починаючи від статей новин до технічних статей.

Вірус Stuxnet

Витік даних Marriott

Витік даних Організації Об'єднаних Націй

Витік бази даних підтримки клієнтів корпорації Майкрософт

Витік даних медичних досліджень

Примітка: Ви можете використовувати веб-браузер у віртуальній машині, встановленій у попередній лабораторній роботі для вивчення проблем, пов'язаних з безпекою. Використовуючи віртуальну машину ви запобігаєте встановленню шкідливого ПЗ на вашому комп'ютері.

b. Прочитайте статті, знайдені вами на кроці 1a і будьте готові обговорити і поділитися своїми дослідженнями щодо того, хто, що, коли, де і чому про кожну атаку.

Частина 2: Напишіть аналіз кібератаки.

Виберіть одну популярну кібератаку з кроку 1a і напишіть аналіз атаки, що включатиме відповіді на питання нижче.

Запитання:

a. Хто були жертвами атак?

b. Які технології та інструменти використовувалися під час нападу?

c. Коли сталася атака в мережі?

d. Які системи були метою?

e. Якою була мотивація нападників у цьому випадку? Що вони сподіваються досягти?

f. Яким був результат нападу? (викрадені дані, викуп, пошкодження системи тощо)

Рекомендації щодо виконання роботи

Довідкова інформація / Сценарій

Обчислювальні потужність та ресурси надзвичайно зросли за останні 10 років. Вигода від використання багатоядерних процесорів і великої кількості ОЗП - це можливість використовувати віртуалізацію. За допомогою віртуалізації один або декілька віртуальних комп'ютерів можуть працювати на одному фізичному комп'ютері. Віртуальні комп'ютери, що працюють на фізичних комп'ютерах, називаються віртуальними машинами Віртуальні машини часто називають гостьовими, а фізичні комп'ютери часто називають хостами. Кожен, хто має сучасний комп'ютер та операційну систему, може запускати віртуальні машини.

Файл образу віртуальної машини створено для встановлення на ваш комп'ютер. У цій роботі ви завантажуєте та імпортуєте цей файл образу за допомогою програми віртуалізації для настільних комп'ютерів, наприклад VirtualBox.

Необхідні ресурси

Комп'ютер з мінімум 8 Гб оперативної пам'яті та 40 Гб вільного місця на диску

Високошвидкісний доступ до мережі Інтернет для завантаження Oracle VirtualBox та файлу образу віртуальної машини

Інструкції

Підготуйте комп'ютер для віртуалізації

У Частині 1 ви завантажите та встановите програмне забезпечення для віртуалізації настільних комп'ютерів, а також завантажите файл образу, який можна використовувати для виконання лабораторних робіт протягом всього курсу. Для цієї лабораторної роботи на віртуальній машині працює Linux.

Завантажте та встановіть VirtualBox.

VMware Workstation Player і Oracle VirtualBox - це дві програми віртуалізації, які можна завантажити та встановити для встановлення файлу образу. У цій роботі ви будете використовувати VirtualBox.

Перейдіть до http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html.

Виберіть і завантажте відповідний файл на основі вашої операційної системи.

Коли ви завантажили інсталяційний файл VirtualBox, запустіть програму встановлення та прийміть установки встановлення за замовчуванням.

Завантажте файл образу для віртуальної машини.

Файл образу був створений відповідно до Відкритого формату віртуалізації (Open Virtualization Format, OVF). OVF є відкритим стандартом для упаковки та розповсюдження віртуальних пристроїв. Пакет OVF містить декілька файлів, розміщених у одному каталозі. Цей каталог потім поширюється як пакет OVA.

Цей пакет містить усі файли OVF, необхідні для розгортання віртуальної машини. Віртуальна машина, що використовується в цій роботі, експортується відповідно до стандарту OVF.

Перейдіть на сторінку CyberOps Associates Virtual Machines на сайті netacad.com.

Скачайте файли образів ***cyberops_workstation.ova*** *і* ***security_onion.ova*** *і* визначте місце розташування завантаженої ВМ.

Імпортування віртуальної машини в Inventory VirtualBox

У частині 2 ви імпортуєте образ віртуальної машини в VirtualBox і запускаєте віртуальну машину.

Імпортуйте файл віртуальної машини в VirtualBox

Відкрийте ***VirtualBox***. Натисніть ***File > Import Appliance...*** для того, щоб імпортувати образ віртуальної машини.

Вкажіть розташування файлу .OVA та натисніть ***Далі***

З'явиться нове вікно з параметрами, запропонованими в архіві OVA. Перегляньте налаштування за замовчуванням і змініть по мірі необхідності. Натисніть ***Імпортувати (Import)*** для продовження.

Коли процес імпорту буде завершено, ви побачите нову віртуальну машину, додану до VirtualBox на лівій панелі. Віртуальна машина тепер готова до використання.

Запустіть віртуальну машину та увійдіть до системи

Виберіть і запустіть щойно імпортовані віртуальні машини. В якості прикладу в цій лабораторній роботі використовується робоча станція CyberOps.

Натисніть на зелену стрілку ***Старт*** у верхній частині вікна програми VirtualBox. Якщо ви отримаєте таке діалогове вікно, натисніть кнопку ***Змінити налаштування мережі*** та встановіть Bridged Adapter (Міст). Натисніть розкривний список поряд з ім'ям та виберіть мережевий адаптер (буде відрізнятися для кожного комп'ютера).

- ***Примітка:*** якщо в мережі не налаштований DHCP, натисніть кнопку ***Змінити налаштування мережі*** та виберіть ***NAT*** у спадному списку. Параметри мережі також можуть бути доступні через ***Параметри*** в Oracle VirtualBox Manager або в меню віртуальної машини, виберіть ***Devices >Network > Network Settings***. Можливо, потрібно буде вимкнути та ввімкнути мережевий адаптер, щоб зміни вступили в силу.

Натисніть **OK** Відкриється нове вікно, і стартує процес завантаження віртуальної машини.

Коли процес завантаження завершено, віртуальна машина запитає ім'я користувача та пароль. Для входу в віртуальну машину використовуйте такі облікові дані:

Ім'я користувача: ***analyst***

Пароль: ***cyberops***

Вам буде представлено середовище: у нижній частині панелі запуску, піктограми на робочому столі та меню програми вгорі.

Примітка: Зверніть увагу на фокус клавіатури та миші. Коли ви натискаєте вікно віртуальної машини, миша та клавіатура працюватимуть на гостьовій

операційній системі. Ваша операційна система не буде визначати натискання клавіш або рухів миші. Натисніть праву клавішу **CTRL**, щоб повернути фокус клавіатури та миші в операційну систему хоста.

Ознайомтеся з віртуальною машиною

Щойно встановлену віртуальну машину можна використовувати для виконання багатьох лабораторних робіт у цьому курсі. Ознайомтеся з піктограмами в списку нижче:

Значки панелі запуску (зліва направо):

Показати робочий стіл

Відкрити термінал

Застосунок для роботи з файловою системою

Застосунок веб-браузера (Firefox)

Інструмент пошуку

Домашній каталог поточного користувача

Всі програми, пов'язані з курсом, знаходяться в ***Applications Menu > CyberOPs***.

Перелічіть програми в меню CyberOPs.

Запишіть тут свою відповідь.

Відкрийте ***Terminal Emulator*** Введіть команду ***ip address*** у відповідь на запит, щоб визначити IP-адресу вашої віртуальної машини.

Запитання:

- Які IP-адреси призначені для вашої віртуальної машини?

Знайдіть і запустіть програму веб-браузера.

Запитання:

- Чи можете ви перейти до своєї улюбленої пошукової системи?

Вимкніть VM (Shut down).

Коли ви закінчите роботу з віртуальною машиною, ви можете зберегти стан віртуальної машини для подальшого використання або вимкнути віртуальну машину.

Закриття віртуальної машини за допомогою графічного інтерфейсу користувача:

- У пункті **File** меню Virtual Box, виберіть **Закрити (Close)**...
- Натисніть перемикач ***Зберегти стан машини (Save the machine state)*** та натисніть **OK**. Під час наступного запуску віртуальної машини ви зможете відновити роботу з операційною системою у поточному стані, який запам'ятали.
-

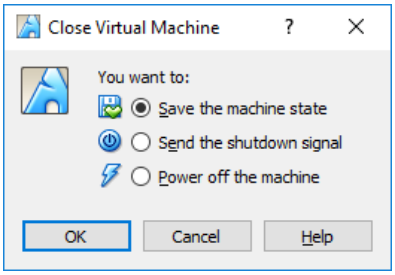

Рисунок 2. – Закриття віртуальної машини

- Іншими двома опціями є:
- Send the shutdown signal**: *імітує надсилання сигналу завершення на фізичному комп'ютері***
- Power off the machine**: *імітує сигнал вимкнення живлення на фізичному комп'ютері***

Закриття віртуальної машини за допомогою графічного інтерфейсу користувача:

- Щоб вимкнути віртуальну машину за допомогою командного рядка, можна скористатися пунктами меню всередині віртуальної машини або ввести команду ***sudo shutdown -h now*** у вікні терміналу і надати пароль **cyberops** під час запиту.

Перезавантаження VM:

- Якщо ви хочете перезавантажити віртуальну машину, ви можете скористатися пунктами меню всередині віртуальної машини або ввести команду ***sudo reboot*** в терміналі і надати пароль ***cyberops*** під час доступу.

Примітка: Ви можете використовувати веб-браузер у цій віртуальній машині для дослідження проблем безпеки. Використовуючи віртуальну машину ви запобігаєте встановленню шкідливого ПЗ на вашому комп'ютері.

Вимоги до звіту

Звіт по роботі повинен містити:

1. Назву дисципліни та лабораторної роботи.
2. Прізвище, ім’я та по батькові студента, код групи.
4. Знімки зображень екрану, які коментують виконання завдань.
5. Коментарі до кожного етапу.
5. Висновки.

Контрольні питання і завдання

1. Хто були жертвами атак?
2. Які технології та інструменти використовувалися під час нападу?
3. Коли сталася атака в мережі?
4. Які системи були метою?
5. Якою була мотивація нападників у цьому випадку? Що вони сподіваються досягти?
6. Яким був результат нападу? (викрадені дані, викуп, пошкодження системи тощо)

2.2 Лабораторна робота № 2
Дослідження вразливостей та інцидентів кібербезпеки

Об’єкт: вразливості та інциденти кібербезпеки.

Мета: дослідження та аналіз інцидентів кібербезпеки. Проведення пошуку сертифікації. Дослідження наявних вакансій у сфері кібербезпеки. Дослідження та аналіз уразливості програм IoT.

Стислі теоретичні відомості

Дослідження та аналіз інцидентів кібербезпеки.

ФБР підрахувало, що кіберзлочинність коштувала фізичним особам і компаніям понад 3,5 мільярда доларів у 2019 році. Уряди, підприємства та окремі користувачі все частіше стають об'єктами кібератак та інцидентів кібербезпеки.

У цій лабораторній роботі ви створите трьох гіпотетичних кібер-зловмисників, у кожного з яких є ціллю організація, тип атаки та мотив. Крім того, запропонуєте метод, за допомогою якого організація може запобігти або пом'якшити атаку.

Примітка: Для пошуку інформації про проблеми безпеки можна використовувати веб-переглядач на віртуальній машині, встановленій під час попередньої лабораторної роботи. Використовуючи віртуальну машину ви запобігаєте встановленню шкідливого ПЗ на вашому ком'ютері.

Потрібно

Сценарій 1

a. Хто нападник?

b. З якою організацією або групою пов'язаний нападник, якщо така є?

c. У чому полягав мотив нападника?

d. Який метод атаки був використаний?

e. Що було ціллю та яка вразливість використовувалися проти бізнесу?

f. Як можна запобігти або пом'якшити цю атаку?

Сценарій 2

a. Хто нападник?

b. З якою організацією/групою пов'язаний нападник?

c. У чому полягав мотив нападника?

d. Який метод атаки був використаний?

e. Що було ціллю та яка вразливість використовувалися проти бізнесу?

f. Як можна запобігти або пом'якшити цю атаку?

Сценарій 3

a. Хто нападник?

b. З якою організацією/групою пов'язаний нападник?

c. У чому полягав мотив нападника?

d. Який метод атаки був використаний?

e. Що було ціллю та яка вразливість використовувалися проти бізнесу?

f. Як можна запобігти або пом'якшити цю атаку?

Проведення пошуку сертифікації та дослідження наявних вакансій в сфері кібербезпеки.

У нашому технологічно-орієнтованому світі, коли світ стає більш пов'язаним, він також стає менш безпечним. Кібербезпека є однією з найбільш швидко зростаючих і затребуваних професій. Особи в цій сфері виконують широкий спектр робочих завдань, включаючи, але не обмежуючись ними, послуги з консультацій, розслідувань та управління програмами для зменшення ризиків через внутрішні та зовнішні джерела. Фахівці з кібербезпеки зобов'язані оцінювати, розробляти та впроваджувати плани безпеки, проводити глибоке розслідування шахрайства, проводити дослідження безпеки та оцінювати ризики і пропонувати рішення щодо потенційних порушень безпеки.

Особи з хорошими навичками безпеки мають великий потенціал збільшення заробітку. Щоб бути кандидатом для одного з цих високооплачуваних робочих місць, необхідно мати належну кваліфікацію. Для цього важливо враховувати галузеві сертифікати, доступні для цієї кар'єри. Є багато сертифікацій на вибір. Вибір правильних сертифікацій для Вас вимагає ретельного розгляду.

Примітка: Для пошуку інформації про проблеми безпеки можна використовувати веб-переглядач на віртуальній машині, встановленій під час попередньої лабораторної роботи. Використовуючи віртуальну машину, ви запобігаєте встановленню шкідливого ПЗ на вашому ком'ютері.

Потрібно

Проведіть пошук Сертифікацій.

a. Використовуйте свою улюблену пошукову систему, щоб знайти найпопулярніші сертифікації, пов'язані з кібербезпекою. Перерахуйте їх нижче разом з назвою організації, яка надає сертифікацію.

b. Виділіть три сертифікати зі списку вище та надайте більш детальну інформацію про сертифікаційні вимоги/знання, отримані, наприклад: специфічні чи нейтральні постачальники, кількість іспитів для отримання сертифікату, вимоги до іспитів, обговорювані теми тощо.

Дослідіть наявні вакансії в кібербезпеці

Indeed.com є одним з найбільших сайтів з пошуку роботи у всьому світі. Використовуючи свій вибір, перейдіть до glassdoor.com і знайдіть робочі місця з кібербезпеки, доступні протягом останніх двох тижнів. Налаштуйте пошук так, як вам хотілося б. Ви можете шукати вакансії в своєму районі або області, в якій ви хотіли б жити і працювати.

Запитання:

a. Скільки нових списків вакансій було розміщено протягом останніх двох тижнів?

b. Який діапазон заробітної плати для топ-10 оголошень?

c. Які найбільш поширені кваліфікації потрібні роботодавцям?

d. Які галузеві сертифікації потрібні цим роботодавцям?

e. Чи відповідають сертифікати для вакансій, вказаним в кроці 1a?

f. Досліджуйте інтернет-ресурси, які дозволять вам легально перевірити свої навички злому. Ці інструменти дозволяють новачкам із обмеженим досвідом кібербезпеки удосконалити свої навички тестування на проникнення. Одним з таких сайтів є Google Gruyere (веб-застосунки експлойтів і захисту). Які проблеми ви можете знайти?

Дослідження та аналіз уразливості програм IoT.

Інтернет речей (IoT) складається з цифрових підключених пристроїв, які з'єднують кожен аспект нашого життя, включаючи наші будинки, офіси, автомобілі і навіть наші тіла в Інтернет. З прискореним впровадженням IPv6 і майже універсальним розгортанням мереж Wi-Fi, IoT зростає експоненціальними темпами. Експерти оцінюють, що до 2030 року кількість активних пристроїв IoT буде наближатися до 50 мільярдів.

Однак, IoT пристрої є особливо вразливими до загроз безпеці, оскільки безпека не завжди розглядається в процесі розробки продукту IoT. Крім того, пристрої IoT часто продаються зі старими та невиправленими вбудованими операційними системами та програмним забезпеченням.

Потрібно

Проведіть пошук вразливостей застосунків IoT

Використовуючи улюблену пошукову систему, виконайте пошук уразливостей Інтернету речей (IoT). Під час пошуку знайдіть приклад

уразливості IoT для кожного з напрямків IoT: промисловість, енергетичні системи, охорона здоров'я та уряд. Будьте готові обговорити, хто може скористатися цією вразливістю і чому та що викликало вразливість, і що можна зробити, щоб обмежити вразливість?

Примітка: Для пошуку інформації про проблеми безпеки можна використовувати веб-переглядач на віртуальній машині, встановленій під час попередньої лабораторної роботи. Використовуючи віртуальну машину ви запобігаєте встановленню шкідливого ПЗ на вашому ком'ютері.

З вашого дослідження виберіть уразливість IoT і дайте відповіді на такі запитання:

Запитання:

a. У чому полягає вразливість?

b. Хто може її використовувати? Поясніть.

c. Чому існує вразливість?

d. Що можна зробити, щоб обмежити вразливість?

Вимоги до звіту

Звіт по роботі повинен містити:

1. Назву дисципліни та лабораторної роботи.
2. Прізвище, ім’я та по батькові студента, код групи.
4. Відповіді на запитання кожного етапу.
5. Коментарі до кожного етапу.
5. Висновки.

Контрольні питання і завдання

Наведені в кожному сценарії виконання лабораторної роботи.

2.3 Лабораторна робота № 3
Процеси та застосунки Windows для дослідження функцій маршрутизації та реєстру

Об'єкт: процеси та застосунки Windows.

Мета: вивчити процеси, програми та застосунки, які виконуються. Досліджувати процеси за допомогою засобу Process Explorer у Windows Sysinternals Suite.

Стислі теоретичні відомості

Визначення запущених процесів

Завантаження Windows Sysinternals Suite.

Запуск TCP/UDP Endpoint Viewer.

Дослідження запущених процесів.

Вивчення процесів, які запустив користувач.

Завантаження Windows Sysinternals Suite.

Перейдіть за наступним посиланням для завантаження Windows Sysinternals Suite:

https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Після завершення завантаження натисніть правою кнопкою миші на zip-файлі та оберіть **Extract All…**, для вилучення файлів з папки. Оберіть назву за замовчуванням та призначення у папці Завантаження і натисніть **Extract**.

Вийдіть з веб-браузера.

Запуск TCP/UDP Endpoint Viewer.

Перейдіть до папки SysinternalsSuite з усіма видобутими файлами.

Відкрийте **Tcpview.exe**. Прийміть ліцензійну угоду Process Explorer, коли з'явиться запит. Натисніть **Yes** аби дозволити цій програмі робити зміни на вашому пристрої.

Вийдіть з Провідника і закрийте всі запущені програми.

Дослідження запущених процесів.

TCPView показує поточні процеси на вашому Windows ПК. Зараз запущені лише процеси Windows.

Двічі клацніть на **lsass.exe**.

Що таке lsass.exe? У якій теці розташовано цей файл?

Після завершення закрийте вікно властивостей lsass.exe.

Перегляньте властивості інших запущених процесів.

Примітка: Не всі процеси можуть надавати інформацію про властивості у відповідь на запит.

Вивчення процесів, які запустив користувач.

Відкрийте веб-браузер, наприклад Microsoft Edge.

Що можна побачити у вікні TCPView window?

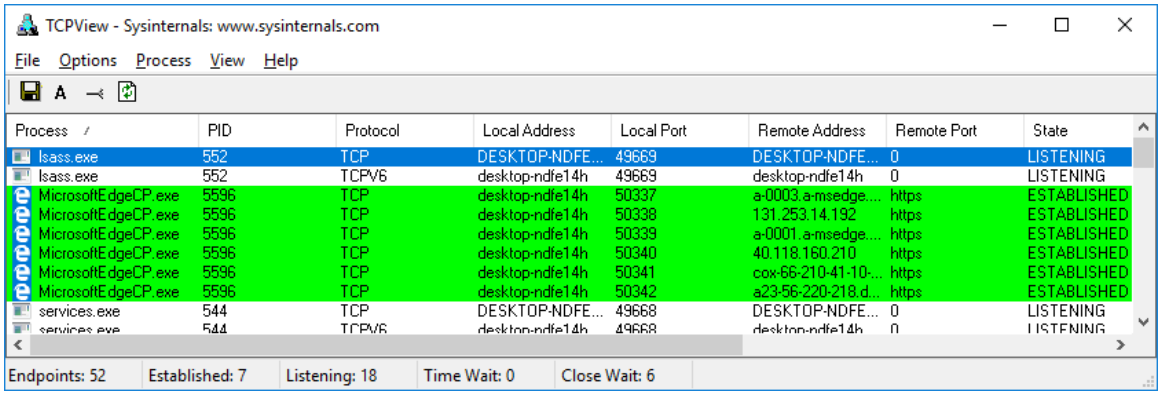

Рисунок 1 – TCPView

Закрийте веб-браузер.

Процеси веб-браузера будуть видалені з вікна TCPView window.

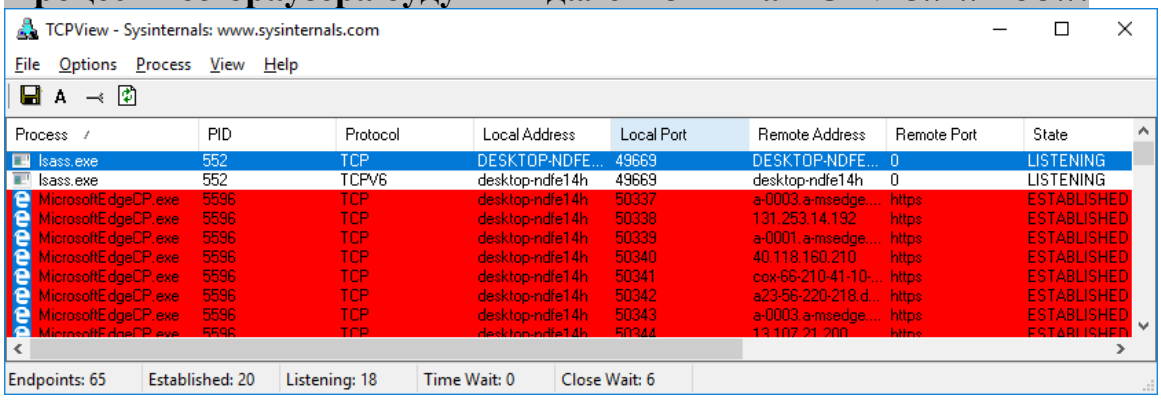

Рисунок 2 – TCPView після запуску браузеру

Повторно відкрийте веб-браузер. Дослідіть деякі процеси, наведені у вікні TCPView. Запишіть отримані дані.

Дослідження процесів, потоків, дескрипторів і реєстру Windows

Дослідження процесів

Процеси - це програми або застосунки, які виконуються. Ви будете досліджувати процеси за допомогою засобу Process Explorer у Windows SysInternals Suite. Також, ви запустите та будете спостерігати за новими процесами.

Завантажте Windows Sysinternals Suite.

Перейдіть за наступним посиланням для завантаження Windows SysInternals Suite: https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Після завершення завантаження розпакуйте файли з теки.

Залиште веб-браузер відкритим для виконання наступних кроків.

Дослідіть активний процес.

Перейдіть до теки SysinternalsSuite з усіма розпакованими файлами.

Відкрийте **procexp.exe**. Прийміть ліцензійну угоду Process Explorer, коли з'явиться запит.

Process Explorer відображає список активних на даний момент процесів.

Щоб знайти процес веб-браузера, перетягніть значок **Find Window's Process (Процес у вікні пошуку)** у відкрите вікно браузера. У цьому прикладі було використано Microsoft Edge.

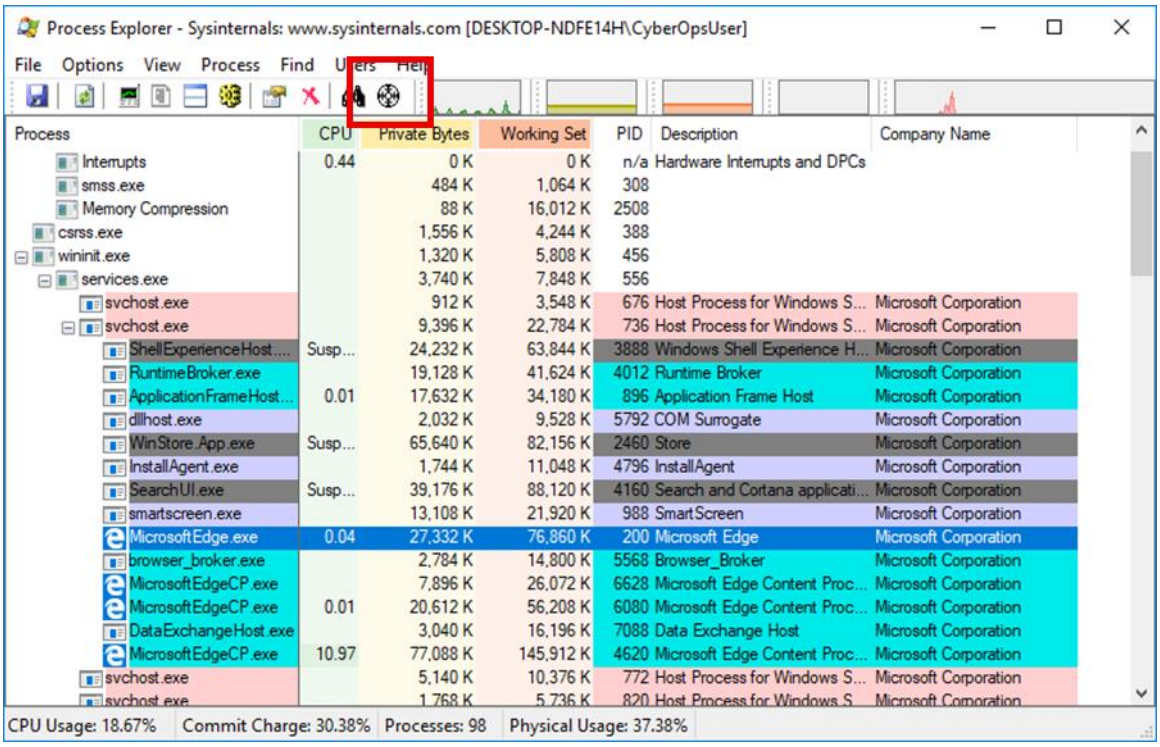

Рисунок 3 – Process Explorer

Процес Microsoft Edge можна завершити в Process Explorer. Натисніть правою кнопкою миші вибраний процес і оберіть **Kill Process(Знищити процес)**. Натисніть **OK**, щоб продовжити.

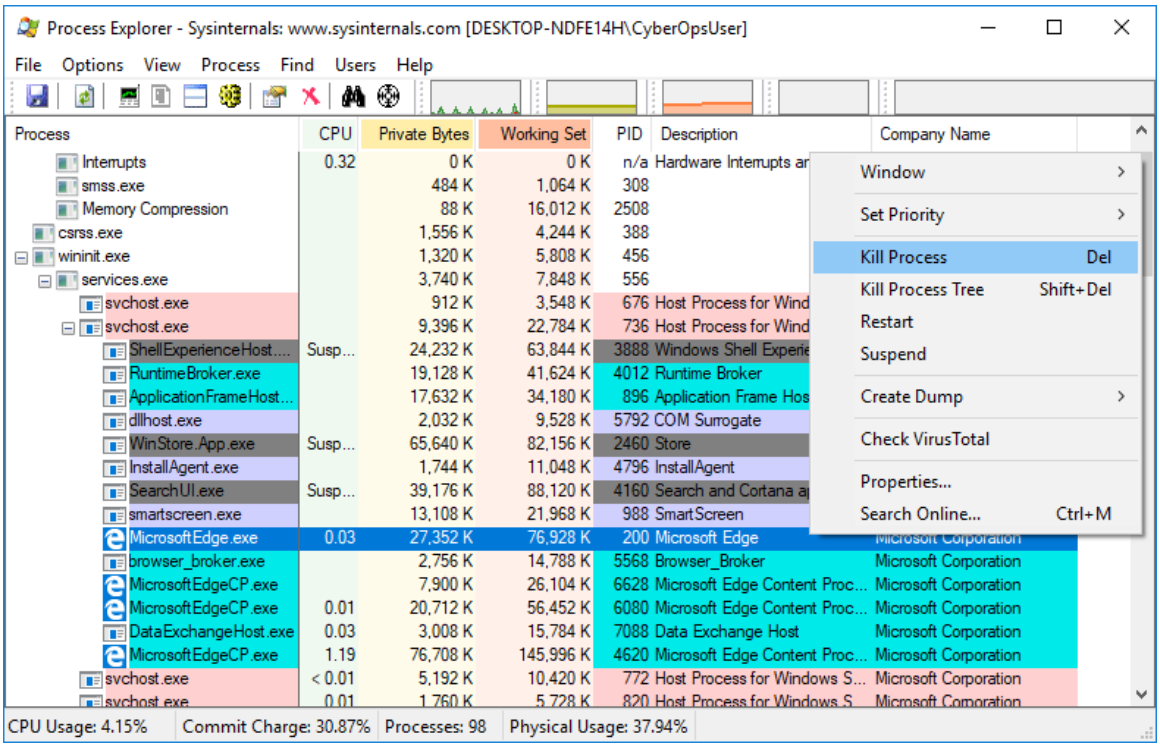

Рисунок 4 – Знищення процесу в Process Explorer

Що сталося з вікном веб-браузера, коли процес був знищений?

Почніть інший процес.

Відкрийте командний рядок (Command Prompt). (**Пуск** > Пошук **Командний рядок** > виберіть **Командний рядок**)

Перетягніть піктограму **Find Window's Process (Процес у вікні пошуку)** у вікно командного рядка та знайдіть виділений процес командного рядка в Process Explorer.

Процесом для командного рядка є cmd.exe. Його батьківський процес – процес explorer.exe. У cmd.exe є дочірній процес conhost.exe.

Перейдіть до вікна командного рядка. Запустіть ping та спостерігайте за змінами процесу cmd.exe.

Що відбулося під час процесу ping?

Переглядаючи список активних процесів, ви виявите, що дочірній процес conhost.exe може бути підозрілим. Щоб перевірити наявність шкідливого вмісту, натисніть правою кнопкою миші **conhost.exe** і виберіть **Check VirusTotal**. Коли з'явиться запит, натисніть **Yes**, щоб прийняти Умови використання VirusTotal. Потім натисніть **OK** для наступного запрошення.

Розгорніть вікно Process Explorer або прокрутіть вправо, доки не відобразиться стовпець VirusTotal. Натисніть посилання під стовпцем VirusTotal. Веб-браузер за замовчуванням відкривається з результатами щодо шкідливого вмісту conhost.exe.

Натисніть правою кнопкою миші на cmd.exe і виберіть **Kill Process**.

Що сталося з дочірнім процесом conhost.exe?

Дослідження потоків і дескрипторів

У цій частині ви досліджуватимете потоки та дескрипторів. Процеси мають один або кілька потоків. Потік – це одиниця виконання в процесі. Дескриптор – це абстрактне посилання на блоки пам'яті або об'єкти, якими керує операційна система. Ви будете використовувати Process Explorer (procexp.exe) у Windows SysInternals Suite, щоб досліджувати потоки та дескриптори.

Дослідіть потоки.

Відкрийте командний рядок (Command Prompt).

У вікні Process Explorer натисніть правою кнопкою миші conhost.exe і виберіть **Properties…**.. Натисніть вкладку **Threads** , щоб переглянути активні потоки для процесу conhost.exe. Натисніть **OK** , щоб продовжити, якщо з'явиться діалогове вікно з попередженням.

Розгляньте деталі потоку.

Який тип інформації доступний у вікні Properties?

Натисніть **OK**, щоб продовжити.

Дослідіть дескриптори.

У Process Explorer натисніть **View** > виберіть **Lower Pane View** > **Handles** , щоб переглянути дескриптори, пов'язані з процесом conhost.exe.

Дослідіть дескриптори. На що вказують дескриптори?

Закрийте Process Explorer, коли закінчите.

Вивчення реєстру Windows

Реєстр Windows – це ієрархічна база даних, яка зберігає більшість параметрів конфігурації операційних систем і середовища робочого столу.

Щоб отримати доступ до реєстру Windows, натисніть **Пуск** > Пошук **regedit** і виберіть **Registry Editor**. Натисніть **Yes** аби дозволити програмі робити зміни на вашому пристрої.

Registry Editor (Редактор реєстру) має п'ять гілок. Ці гілки знаходяться у верхньому рівні реєстру.

HKEY_CLASSES_ROOT фактично підключ класів HKEY_LOCAL_MACHINE\Software\. Він зберігає інформацію, яку використовують зареєстровані програми, як-от зіставлення розширень файлів, а

також дані програмного ідентифікатора (ProgID), ідентифікатора класу (CLSID) та ідентифікатора інтерфейсу (IID).

HKEY_CURRENT_USER містить налаштування та конфігурації для користувачів, які в даний момент увійшли в систему.

HKEY_LOCAL_MACHINE зберігає інформацію про конфігурацію, специфічну для локального комп'ютера.

HKEY_USERS містить налаштування та конфігурації для всіх користувачів на локальному комп'ютері. HKEY_CURRENT_USER є підключем HKEY_USERS.

HKEY_CURRENT_CONFIG зберігає інформацію про обладнання, яка використовується під час завантаження локальним комп'ютером.

На попередньому кроці ви прийняли Ліцензійну угоду для Process Explorer. Перейдіть до ключа реєстру EulaAccepted для Process Explorer.

Натисніть, щоб вибрати Process Explorer у **HKEY_CURRENT_USER** > **Software** > **Sysinternals** > **Process Explorer**. Прокрутіть донизу, щоб знайти ключ **EulaAccepted**. Наразі значення для ключа реєстру EulaAccepted становить 0x00000001(1).

Двічі натисніть ключ реєстру **EulaAccepted** . Наразі значення data встановлено на 1. Значення 1 вказує на те, що ліцензійна угода була прийнята користувачем.

Змініть значення **1** на **0** для значення даних. Значення 0 вказує на те, що Ліцензійну угоду не було прийнято. Натисніть **OK**, щоб продовжити.

Що таке значення для цього ключа реєстру в стовпці дані?

Відкрийте **Process Explorer**. Перейдіть до теки, куди ви завантажили SysInternals. Відкрийте теку **SysInternalsSuite** > Відкрийте **procexp.exe**.

Коли ви відкривали Process Explorer, що ви бачили?

Створення нового облікового запису локального користувача. Перегляд властивостей облікового запису користувача. Зміна облікових записів локальних користувачів.

Створення нового облікового запису локального користувача

Відкрийте Інструмент облікових записів користувача.

Увійдіть у комп'ютер з обліковим записом адміністратора. В цьому прикладі використовується обліковий запис **CyberOpsUser**.

Натисніть **Пуск**> пошук **Панель управління**. Виберіть **Облікові записи користувачів** в поданні Маленькі значки. Щоб змінити вигляд, виберіть у вікні "Перегляд" випадаюче меню **Малі значки**.

Створіть обліковий запис користувача.

У вікні **Облікові записи користувачів** > натисніть **Керувати іншим обліковим записом**.

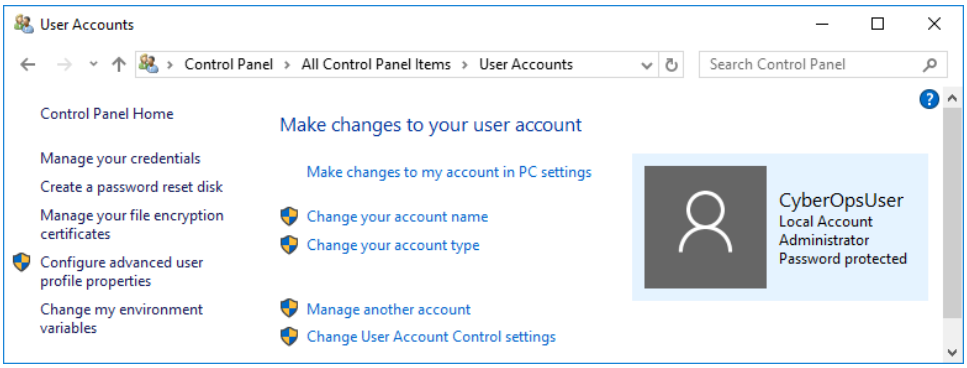

Рисунок 5 – Керування іншим обліковим записом

У вікні **Керування обліковими записами** натисніть кнопку **Додати нового користувача в параметрах ПК**.

У вікні **Настройки** натисніть **Додати когось іншого на цей комп'ютер**.

У вікні **Як ця особа входитиме в обліковий запис** натисніть **У мене немає облікових даних цієї особи**.

У вікні **Створення облікового запису**, що відкриється, натисніть кнопку **Додати користувача без облікового запису Microsoft**.

У вікні **Створення користувача для цього ПК введіть** необхідну інформацію для створення нового облікового запису користувача з ім’ям **User1**. Натисніть **Далі**, щоб створити новий обліковий запис користувача.

Який тип профілю користувача ви тільки що створили?

Увійдіть до новоствореного облікового запису користувача. Вхід повинен бути успішним.

Перейдіть до папки **C:\Users**. Натисніть правою кнопкою миші теку **User1** і виберіть **Властивості**, а потім перейдіть на вкладку **Безпека**.

Які групи або користувачі повністю контролюють цю папку?

Відкрийте теку, яка належить CyberOpsUser. Натисніть правою кнопкою миші теку і перейдіть на вкладку **Властивості**.

Ви змогли отримати доступ до теки? Поясніть.

Вийдіть з облікового запису User1. Увійдіть в систему як CyberOpsUser.

Перейдіть до теки **C:\Users**. Натисніть правою кнопкою миші на теці та виберіть **Властивості**. Натисніть вкладку **Безпека**.

Які групи або користувачі повністю контролюють цю теку?

Перегляд властивостей облікового запису користувача

Натисніть **Пуск**> Пошук за **Панель управління**> Вибрати **Адміністративні інструменти**> Вибрати **Керування комп'ютером**.

Виберіть **Локальні користувачі та групи**. Натисніть на теці **Користувачі**.

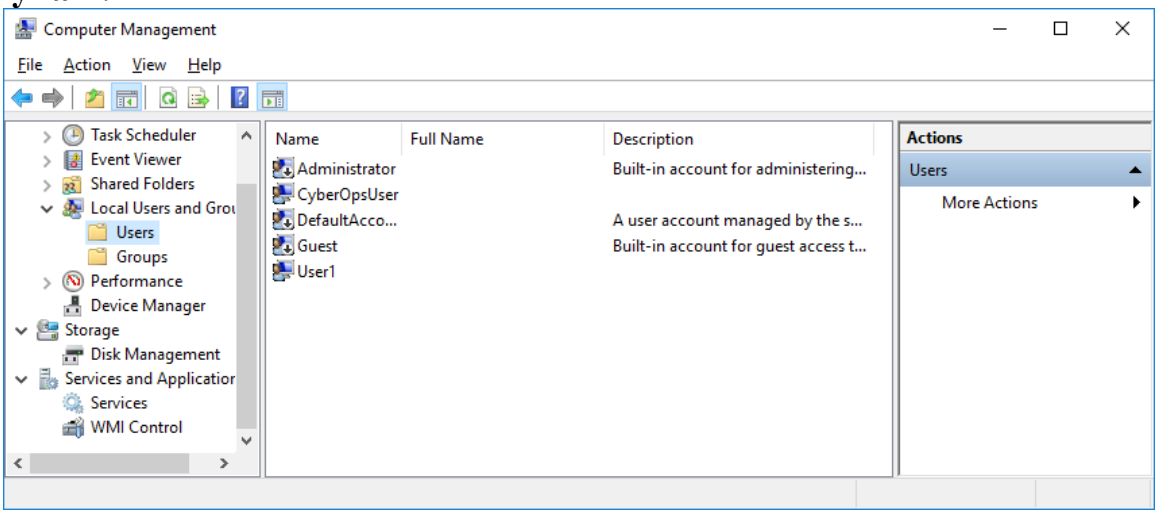

Рисунок 6 – Властивості груп облікових записів

Натисніть правою кнопкою миші **User1** і виберіть **Властивості**.

Відкрийте вкладку **Членство в групах**.

В яку групу входить User1?

Натисніть правою кнопкою миші обліковий запис **CyberOpsUser** та виберіть **Властивості**.

В яку групу входить цей користувач?

Змінення локальних облікових записів користувачів

Змінити тип облікового запису.

Перейдіть на **Панель керування** та виберіть **Облікові записи користувачів** . Натисніть **Керувати іншим обліковим записом**. Виберіть **User1**.

У вікні «Змінити обліковий запис» натисніть обліковий запис **User1**. Натисніть **Змінити тип облікового запису**.

Виберіть перемикач **Адміністратор**. Натисніть **Змінити тип облікового запису**.

Тепер обліковий запис User1 має адміністративні права.

Перейдіть до **Панель керування**> **Адміністративні інструменти**> **Керування комп'ютером**. Натисніть **Локальні користувачі та групи**> **Користувачі**.

Натисніть правою кнопкою миші **User1** і виберіть **Властивості**. Натисніть **Учасник**.

До яких груп належить User1?

Виберіть **Адміністратори** та натисніть **Видалити**, щоб видалити User1 з Administrative group. Натисніть **OK**, щоб продовжити.

Видаліть обліковий запис.

Щоб видалити обліковий запис, натисніть правою кнопкою миші **User1** та виберіть **Delete**.

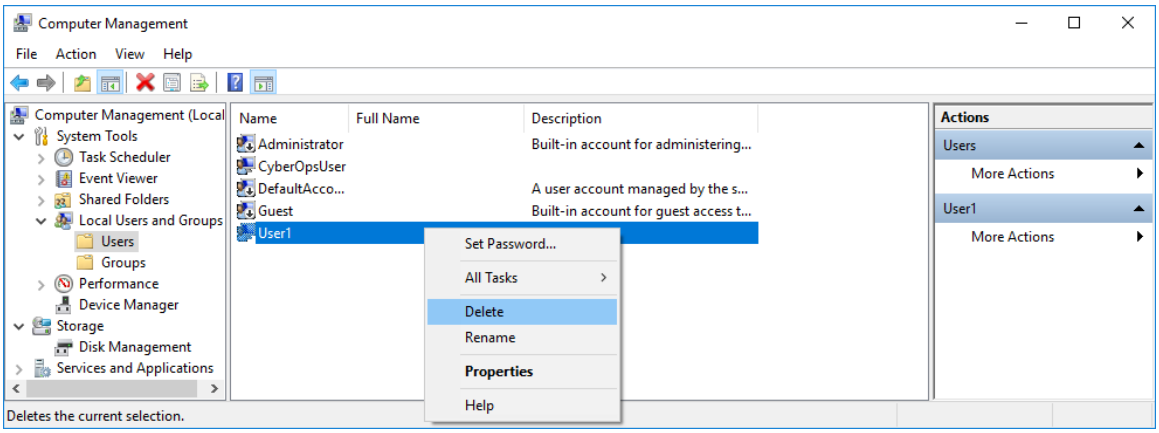

Рисунок 7 – Видалення облікових записів

Натисніть **OK**, щоб підтвердити видалення.

Як ще можна видалити обліковий запис користувача?

Питання для самоперевірки

Чому важливо захистити всі облікові записи за допомогою сильних паролів?

Навіщо вам створювати користувача зі стандартними привілеями?

Доступ до консолі PowerShell. Дослідження команд командного рядка та PowerShell. Дослідження з командлетів. Дослідження команди netstat за допомогою PowerShell. Очищення кошика за допомогою PowerShell.

Довідкова інформація

PowerShell - потужний інструмент автоматизації. Це і командна консоль, і мова сценаріїв. У цій лабораторній роботі ви будете використовувати консоль для виконання деяких команд, доступних як у командному рядку, так і в PowerShell. PowerShell також має функції, які можуть створювати скрипти для автоматизації завдань та роботи разом із операційною системою Windows.

Доступ до консолі PowerShell.

Натисніть **Пуск**. Знайдіть і виберіть **powerhell**.

Натисніть **Пуск**. Знайдіть і виберіть **Командний рядок**.

Дослідження команд командного рядка та PowerShell.

Введіть **dir** в запрошенні в обох вікнах.

Які вихідні дані команди **dir**?

Спробуйте іншу команду, яку ви використали в командному рядку, наприклад **ping**, **cd** та **ipconfig**.

Які результати ви отримали?

Дослідження командлетів

Команди PowerShell, командлети, конструюються у вигляді рядка *дієслово-іменник*. Щоб визначити команду PowerShell для виведення списку підкаталогів і файлів в каталозі, введіть **Get-Alias dir** в запрошенні PowerShell.

PS C:\Users\CyberOpsUser> **Get-Alias dir**

CommandTypeNameVersionSource

Aliasdir -> Get-ChildItem

Яка команда PowerShell для **dir** ?

Щоб отримати докладнішу інформацію про командлети, виконайте пошук командлетів **Microsoft powershell cmdlets** в Інтернеті.

Закрийте вікно командного рядка після завершення.

Дослідження команди netstat за допомогою PowerShell.

У запрошенні PowerShell введіть **netstat -h** , щоб переглянути доступні параметри для команди **netstat**.

PS C:\Users\CyberOpsUser> **netstat -h**

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-a Displays all connections and listening ports.

-b Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [ ] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.

<some output omitted>

Щоб відобразити таблицю маршрутизації з активними маршрутами, введіть **netstat -r** в рядку.

PS C:\Users\CyberOpsUser> **netstat -r**

==========

Interface List

3...08 00 27 a0 c3 53 .....Intel(R) PRO/1000 MT Desktop Adapter

```
 10...08 00 27 26 c1 78 ......Intel(R) PRO/1000 MT Desktop Adapter #2
  1...........................Software Loopback Interface 1
===========================================================

IPv4 Route Table
===========================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.5 25
        127.0.0.0 255.0.0.0 On-link 127.0.0.1 331
        127.0.0.1 255.255.255.255 On-link 127.0.0.1 331
  127.255.255.255 255.255.255.255 On-link 127.0.0.1 331
      169.254.0.0 255.255.0.0 On-link 169.254.181.151 281
  169.254.181.151 255.255.255.255 On-link 169.254.181.151 281
  169.254.255.255 255.255.255.255 On-link 169.254.181.151 281
      192.168.1.0 255.255.255.0 On-link 192.168.1.5 281
      192.168.1.5 255.255.255.255 On-link 192.168.1.5 281
    192.168.1.255 255.255.255.255 On-link 192.168.1.5 281
        224.0.0.0 240.0.0.0 On-link 127.0.0.1 331
        224.0.0.0 240.0.0.0 On-link 192.168.1.5 281
        224.0.0.0 240.0.0.0 On-link 169.254.181.151 281
  255.255.255.255 255.255.255.255 On-link 127.0.0.1 331
  255.255.255.255 255.255.255.255 On-link 192.168.1.5 281
  255.255.255.255 255.255.255.255 On-link 169.254.181.151 281
===========================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================
Active Routes:
 If Metric Network Destination Gateway
  1 331 ::1/128 On-link
  3 281 fe80::/64 On-link
 10 281 fe80::/64 On-link
 10 281 fe80::408b:14a4:7b64:b597/128
                             On-link
  3 281 fe80::dd67:9e98:9ce0:51e/128
                             On-link
  1 331 ff00::/8 On-link
  3 281 ff00::/8 On-link
 10 281 ff00::/8 On-link
===========================================================
Persistent Routes:
  None
```

Яка адреса шлюзу IPv4?

Відкрийте та запустіть другу оболонку PowerShell з підвищеними привілеями. Натисніть **Пуск**. Знайдіть PowerShell і натисніть правою кнопкою миші **Windows PowerShell** та виберіть **Запустити як адміністратор**. Натисніть **Так**, щоб додаток мав змогу вносити зміни на вашому пристрої.

Команда netstat також може відображати процеси, пов'язані з активними з'єднаннями TCP. Введіть **netstat -abno** у відповідь на запит.

PS C:\Windows\system32> **netstat -abno**

Active Connections

```
  Proto Local Address Foreign Address State PID
  TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 756
  RpcSs
 [svchost.exe]
  TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
 Can not obtain ownership information
  TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 444
 Can not obtain ownership information
  TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 440
  Schedule
 [svchost.exe]
  TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 304
  EventLog
 [svchost.exe]
  TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 1856
 [spoolsv.exe]
  TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 544
<some output omitted>
```

Відкрийте диспетчер задач. Перейдіть на вкладку **Деталі**. Натисніть заголовок **PID** , щоб упорядковати PID.

Виберіть один з PID з результатів netstat -abno. В цьому прикладі використовується PID 756.

Знайдіть вибраний PID у диспетчері задач. Натисніть правою кнопкою миші вибраний PID у диспетчері завдань, щоб відкрити діалогове вікно **Властивості** для отримання додаткової інформації.

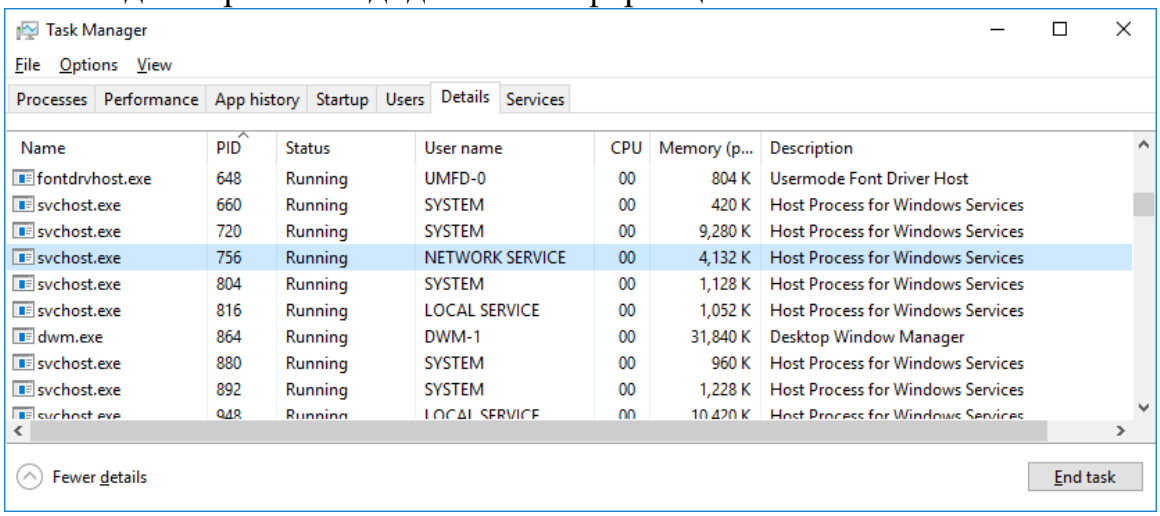

Рисунок 8 – Отримання додаткової інформації

Яку інформацію ви можете отримати на вкладці «Деталі» та діалоговому вікні «Властивості» для вибраного PID?

Звільнення кошика, використовуючи PowerShell.

Команди PowerShell можуть спростити управління великою комп'ютерною мережею. Наприклад, якщо ви хочете реалізувати нове рішення безпеки на всіх серверах у мережі, ви можете скористатися командою або сценарієм PowerShell для реалізації та перевірки роботи служб. Ви також можете запускати команди PowerShell, щоб спростити дії, які виконуються в кілька етапів з використанням інструментів графічного робочого столу Windows.

Відкрийте Кошик. Переконайтеся, що є елементи, які можна остаточно видалити з вашого комп'ютера. Якщо ні, відновіть ці файли.

Якщо в кошику немає файлів, створіть кілька файлів, таких як текстовий файл за допомогою Блокнот, та помістіть їх у кошик.

У консолі PowerShell введіть у рядку **clear-recyclebin**.

PS C:\Users\CyberOpsUser> **clear-recyclebin**

Confirm

Are you sure you want to perform this action?

Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y

Вимоги до звіту

Звіт по роботі повинен містити:

1. Назву дисципліни та лабораторної роботи.
2. Прізвище, ім’я та по батькові студента, код групи.
4. Відповіді на запитання кожного етапу.
5. Коментарі до кожного етапу.
6. Висновки.

Контрольні питання і завдання

1. Що таке lsass.exe? У якій теці розташовано цей файл?
2. Що можна побачити у вікні TCPView window?
3. Що сталося з вікном веб-браузера, коли процес був знищений?
4. Що відбулося під час процесу ping?
5. Що сталося з дочірнім процесом conhost.exe?
6. Який тип інформації доступний у вікні Properties?
7. Дослідіть дескриптори. На що вказують дескриптори?
8. Які групи або користувачі повністю контролюють цю папку?
9. В яку групу входить User1?
10. Як ще можна видалити обліковий запис користувача?
11. Чому важливо захистити всі облікові записи за допомогою сильних паролів?
12. Навіщо вам створювати користувача зі стандартними привілеями?
13. Яку інформацію ви можете отримати на вкладці «Деталі» та діалоговому вікні «Властивості» для вибраного PID?

2.4 Лабораторна робота № 4
Ідентифікація серверів на комп’ютері з системою Linux

Об’єкт: операційна система LINUX
Мета: використання Telnet для тестування TCP-служб.

Рекомендації щодо виконання роботи

Рекомендоване обладнання

Віртуальна машина CyberOps Workstation

Сервери

Сервери - це, по своїй суті, програми, що написані для надання конкретної інформації за запитом. Клієнти, які також є програмами, звертаються до сервера, відправляють запит і чекають відповіді сервера. Можна використовувати багато різних клієнт-серверних технологій зв'язку з найпоширенішими IP-мережами. Ця лабораторна робота базується на серверах та клієнтах IP-мережі.

Доступ до командного рядка

Увійдіть до CyberOps Workstation VM як користувач **analyst** з паролем **cyberops**. Обліковий запис **analyst** використовується як приклад облікового запису користувача в цій лабораторній роботі.

Щоб отримати доступ до командного рядка, натисніть піктограму **terminal**, що розташована на панелі Dock внизу екрану віртуальної машини. Відкриється емулятор терміналу.

Рисунок 1 – Відкриття емулятора терміналу

Відображення служб, що працюють в даний час

На даному комп'ютері може працювати велика кількість різних програм, особливо на комп'ютері із операційною системою Linux. Багато програм запускається у фоновому режимі, тому користувачі не можуть одразу ж визначати, які програми запускаються на певному комп'ютері. У Linux запущені програми також називають *процесами*.

Примітка: Результати виконання команди **ps** будуть відрізнятися, оскільки вони будуть залежати від стану вашої CyberOps Workstation VM.

Виконайте команду **ps**, щоб відобразити всі програми, що працюють у фоновому режимі:

```
[analyst@secOps ~]$ sudo ps –elf
[sudo] password for analyst:
F S UID PID PPID C PRI NI ADDR SZ WCHAN STIME TTY TIME CMD
4 S root 1 0 0 80 0 - 2250 SyS_ep Feb27 ?        00:00:00 /sbin/init
```

1 S root 2 0 0 80 0 - 0 kthrea Feb27 ? 00:00:00 [kthreadd]
1 S root 3 2 0 80 0 - 0 smpboo Feb27 ? 00:00:00 [ksoftirqd/0]
1 S root 5 2 0 60 -20 - 0 worker Feb27 ? 00:00:00 [kworker/0:0H]
1 S root 7 2 0 80 0 - 0 rcu_gp Feb27 ? 00:00:00 [rcu_preempt]
1 S root 8 2 0 80 0 - 0 rcu_gp Feb27 ? 00:00:00 [rcu_sched]
1 S root 9 2 0 80 0 - 0 rcu_gp Feb27 ? 00:00:00 [rcu_bh]
1 S root 10 2 0 -40 - - 0 smpboo Feb27 ? 00:00:00 [migration/0]
1 S root 11 2 0 60 -20 - 0 rescue Feb27 ? 00:00:00 [lru-add-drain]
5 S root 12 2 0 -40 - - 0 smpboo Feb27 ? 00:00:00 [watchdog/0]
1 S root 13 2 0 80 0 - 0 smpboo Feb27 ? 1 S root 13 2 0 80 0 - 0 smpboo Feb27 ?
5 S root 14 2 0 80 0 - 0 devtmp Feb27 ? 00:00:00 [kdevtmpfs]
1 S root 15 2 0 60 -20 - 0 rescue Feb27 ? 00:00:00 [netns]
1 S root 16 2 0 80 0 - 0 watchd Feb27 ? 00:00:00 [khungtaskd]
1 S root 17 2 0 80 0 - 0 oom_re Feb27 ? 00:00:00 [oom_reaper]
<some output omitted>

Чому було необхідно запустити команду **ps** з правами root (попередньо запустивши команду **sudo**)?

У Linux програми також можуть викликати інші програми. Команда **ps** також може бути використана для відображення такої ієрархії процесів. Використовуйте параметри **—ejH** для відображення поточного дерева процесів після запуску веб-сервера nginx з підвищеними привілеями.

Примітка: Інформація про процеси для служби nginx виділена. Значення PID будуть різними.

[analyst@secOps ~]$ **sudo /usr/sbin/nginx**
[analyst@secOps ~]$ **sudo ps –ejH**
[sudo] password for analyst:
PID PGID SID TTY TIME CMD
1 1 1 ? 00:00:00 systemd
167 167 167 ? 00:00:01 systemd-journal
193 193 193 ? 00:00:00 systemd-udevd
209 209 209 ? 00:00:00 rsyslogd
210 210 210 ? 00:01:41 java
212 212 212 ? 00:00:01 ovsdb-server
213 213 213 ? 00:00:00 start_pox.sh
224 213 213 ? 00:01:18 python2.7
214 214 214 ? 00:00:00 systemd-logind
216 216 216 ? 00:00:01 dbus-daemon
221 221 221 ? 00:00:05 filebeat
239 239 239 ? 00:00:05 VBoxService
287 287 287 ? 00:00:00 ovs-vswitchd
382 382 382 ? 00:00:00 dhcpcd
387 387 387 ? 00:00:00 lightdm

410 410 410 tty7 00:00:10 Xorg
460 387 387 ? 00:00:00 lightdm
492 492 492 ? 00:00:00 sh
503 492 492 ? 00:00:00 xfce4-session
513 492 492 ? 00:00:00 xfwm4
517 492 492 ? 00:00:00 Thunar
1592 492 492 ? 00:00:00 thunar-volman
519 492 492 ? 00:00:00 xfce4-panel
554 492 492 ? 00:00:00 panel-6-systray
559 492 492 ? 00:00:00 panel-2-actions
523 492 492 ? 00:00:01 xfdesktop
530 492 492 ? 00:00:00 polkit-gnome-au
395 395 395 ? 00:00:00 nginx
396 395 395 ? 00:00:00 nginx
408 384 384 ? 00:01:58 java
414 414 414 ? 00:00:00 accounts-daemon
418 418 418 ? 00:00:00 polkitd
<some output omitted>

Як представляє процес ієрархії команда **ps**?

Як згадувалося раніше, серверами є, по суті, програми, які часто запускаються самою системою під час завантаження. Таке завдання, що виконується сервером, називають *службою (service).* Так веб-сервер надає веб-служби.

Команда **netstat** це чудовий інструмент, який допомагає ідентифікувати мережеві сервери, що працюють на комп'ютері. Потужність **netstat** полягає у її здатності відображати мережеві з'єднання.

Примітка: Ваш результат виконання команди може бути різним залежно від кількості відкритих мережних з'єднань на вашому комп'ютері.

У вікні терміналу наберіть **netstat**

[analyst@secOps ~]$**netstat{**
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 localhost.localdo:48746 localhost.local:wap-wsp ESTABLISHED
tcp 0 0 localhost.localdo:48748 localhost.local:wap-wsp ESTABLISHED
tcp6 0 0 localhost.local:wap-wsp localhost.localdo:48748 ESTABLISHED
tcp6 0 0 localhost.local:wap-wsp localhost.localdo:48746 ESTABLISHED
tcp6 0 0 localhost.local:wap-wsp localhost.localdo:48744 ESTABLISHED
tcp6 0 0 localhost.localdo:48744 localhost.local:wap-wsp ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags Type State I-Node Path
unix 3 [ ] DGRAM 8472 /run/systemd/notify
unix 2 [ ] DGRAM 8474 /run/systemd/cgroups-agent<some output omitted>

Як показано вище, **netstat** повертає багато інформації, коли використовується без опцій. Багато опцій можна використовувати для фільтрації та форматування результатів виводу команди **netstat** , що робить її значно кориснішою.

Використайте **netstat** з опціями **–tunap**, щоб налаштувати результат виводу команди **netstat**. Зверніть увагу, що **netstat** дозволяє об'єднувати декілька опцій під одним символом "**-**".

Інформацію для сервера nginx виділено.

[analyst@secOps ~]$ **sudo netstat -tunap**

[sudo] password for analyst:

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.0:6633 0.0.0.0:* LISTEN 257/python2.7

tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 395/nginx: master

tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN 279/vsftpd

tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 277/sshd: /usr/bin

tcp6 0 0 :::22 :::* LISTEN 277/sshd: /usr/bin

udp 0 0 192.168.1.15:68 0.0.0.0:* 237/systemd-network

У чому полягає дія опцій **–t**, **-u**, **–n**, **–a** та **–p** команди **netstat**? (використайте **man netstat**, щоб відповісти)

Чи є важливим порядок опцій для **netstat**?

Клієнти приєднуються до порту та, використовуючи правильний протокол, запитують інформацію із сервера. Результат команди **netstat**, що наведений вище, відображає ряд сервісів, які прослуховують певні порти. Цікавими колонками є:

- У першій колонці показано, який протокол Layer 4 застосовано (у цьому випадку - UDP або TCP).
- У третій колонці використовується формат **<ADDRESS:PORT>**, щоб відобразити локальну IP-адресу та порт, на яких доступний певний сервер. IP-адреса 0.0.0.0 означає, що сервер зараз слухає всі IP-адреси, налаштовані на комп'ютері.
- У четвертій колонці використовується той самий формат сокетів **<ADDRESS:PORT>**, щоб відобразити адресу та порт пристрою на віддаленому кінці з'єднання. 0.0.0.0:* означає, що жоден віддалений пристрій наразі не використовує з'єднання.
- П'ята колонка відображає стан з'єднання.
- Шоста колонка відображає ідентифікатор процесу (PID), що відповідальний за з'єднання. Також відображає коротке ім'я, пов'язане з процесом.

На підставі результату виконання команди **netstat**, що наведено в пункті (d), яким є протокол Рівня 4, стан з'єднання та PID процесу, що працює на порту 80?

Хоча номери портів - це лише домовленість, чи ви можете здогадатися, яка служба працює на 80 TCP-порті?

Іноді корисно порівнювати інформацію, що надається командами **netstat** та **ps**. Виходячи з результатів пункту (d), відомо, що процес з **PID 395** пов'язаний з 80 портом TCP. В цьому прикладі використовується 395 PID. Використовуючи **ps** та **grep** отримайте список всіх рядків, що виведені у результаті виконання команди **ps**, які містять **PID 395**: Замініть 395 на номер PID для вашого конкретного запущеного екземпляра nginx:

[analyst@secOps ~]$**sudo ps -elf | grep 395**

[sudo] password for analyst:

1 S root 395 1 0 80 0 - 1829 19:33 ? 00:00:00 nginx: master process /usr/bin/nginx

5 S http 396 395 0 80 0 - 1866 19:33 ? 00:00:00 nginx: worker process

0 S analyst 3789 1872 0 80 0 - 1190 19:53 pts/0 00:00:00 grep 395

Як показано вище, команда **ps** передається через команду **grep**, щоб відфільтрувати лише рядки, які містять номер 395. Результат складається з трьох рядків з текстовим обрамленням.

У першому рядку показано процес, що належить користувачеві **root** (третій стовпець), який розпочато іншим процесом із PID 1 (п’ятий стовпець), о 19:33 (дванадцятий стовпець).

У другому рядку показано процес із PID 396, що належить користувачеві **http**, який розпочато за процесом 395, о 19:33.

У третьому рядку показано процес, який належить користувачеві **analyst** і має PID 3789, розпочатий процесом із PID 1872, як команда **grep 395** .

Процес PID 395 - це **nginx**. Як це можна обгрунтувати з викладеного вище?

Що таке **nginx**? Яка його функція? (Використовуйте google, щоб дізнатися про nginx)

Другий рядок показує, що процес 396 належить користувачеві з ім'ям http і для нього процес із номером 395 є батьківським (parent process). Що це означає? Це загальна поведінка?

Чому відображається в останньому рядку grep 395?

Використання Telnet для тестування TCP служб

Telnet є простою програмою віддаленої консолі. Telnet вважається небезпечним, оскільки не забезпечує шифрування. Адміністратори, які вирішили використовувати Telnet для дистанційного керування мережними пристроями та серверами, надають облікові дані для входу на цей сервер, оскільки Telnet буде передавати дані сеансу у вигляді відкритого тексту. Хоча Telnet не рекомендується використовувати як віддалену консольну програму, він може бути дуже корисним для швидкого тестування або збирання інформації про TCP-служби.

Протокол Telnet працює, за замовчуванням, із портом 23, використовуючи TCP-протокол. Однак клієнт **telnet** дозволяє вказати інший порт. Змінюючи порт і підключившись до сервера, клієнт **telnet** дає змогу мережному аналітику швидко оцінити природу певного сервера шляхом прямого зв'язку з ним.

Примітка: Настійно рекомендується використовувати **ssh** як віддалений інструмент консолі замість **telnet**.

У Частині 1 **nginx** був визначений, як такий, що запускався на призначеному TCP-порту 80. Хоча швидкий пошук Google виявив, що **nginx** є спрощеним веб-сервером, але як аналітик може бути впевненим у цьому? Що робити, якщо зловмисник змінив назву програми зловмисного програмного забезпечення на **nginx** щоб воно виглядало як популярний веб-сервер? Використайте **telnet** для під'єднання до локального вузла через порт 80:

```
[analyst@secOps ~]$ telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
```

Натисніть кілька клавіш на клавіатурі. Будь-яка клавіша буде працювати. Після натискання декількох клавіш натисніть ENTER. Нижче наведено повний вивід, включаючи встановлення з'єднання Telnet та натискання випадкових клавіш (у цьому випадку, fdsafsdaf):

```
fdsafsdaf
HTTP/1.1 400 Bad Request
Сервер: nginx/1.16.1
Date: Tue, 28 Apr 2020 20:09:37 GMT
Content-Type: text/html
Content-Length: 173
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.16.1</center>
</body>
</html>
```

Connection closed by foreign host.

Завдяки протоколу Telnet відкрите текстове TCP-з'єднання було встановлено клієнтом Telnet безпосередньо на сервер nginx, прослуховуючи 127.0.0.1 80 TCP порт. Це з'єднання дозволяє нам надсилати дані безпосередньо на сервер. Оскільки nginx є веб-сервером, він не розуміє послідовності випадкових літер, надісланих йому, і повертає помилку у форматі веб-сторінки.

Чому помилка була надіслана як веб-сторінка?

Поки сервер повідомив про помилку та припинив з'єднання, нам вдалося багато що вивчити. Ми дізналися, що:

Nginx з PID 395 справді є веб-сервером.

Ця версія **nginx** є 1.16.1.

Мережний стек нашої CyberOps Workstation VM повністю функціонує до рівня 7.

Не всі сервіси є рівноправними. Деякі сервіси призначені для приймання неформатованих даних і не припиняються, якщо «сміття» вводиться за допомогою клавіатури. Нижче наведено приклад такої послуги:

Дивлячись на виведений раніше **netstat** результат, можна побачити процес, який працює на порту 22. Використовуйте Telnet для приєднання до нього.

TCP порт 22 призначений для сервісу SSH. SSH дозволяє адміністратору безпечно підключатися до віддаленого комп'ютера.

Нижче наведено вивід:

[analyst@secOps ~]$ **telnet 127.0.0.1 22**
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.2
sdfjlskj
Invalid SSH identification string.
Connection closed by foreign host.

Використовуйте Telnet для підключення до порту 68. Що відбувається? Поясніть.

Вимоги до звіту

Звіт по роботі повинен містити:

1. Назву дисципліни та лабораторної роботи.
2. Прізвище, ім’я та по батькові студента, код групи.
4. Відповіді на запитання кожного етапу.
5. Коментарі до кожного етапу.
6. Висновки.

Контрольні питання і завдання

Надати відповіді на питання, що викладені в порядку виконання роботи.

2.5 Лабораторна робота № 5
Відстеження маршруту

Об’єкт: вебінструменти для дослідження маршрутів.

Мета: перевірка доступності мережі за допомогою утиліти Ping. Відстеження маршруту до віддаленого сервера за допомогою утиліти Traceroute. Відстеження маршруту до віддаленого сервера за допомогою веб-інструмента Traceroute.

Стислі теоретичні відомості

Відстеження маршруту призводить до відображення списку всіх пристроїв маршрутизації, через які проходить пакет, коли перетинає мережу від джерела до пункту призначення. Відстеження маршруту зазвичай виконується в командному рядку:

tracert <ім'я вузла призначення або адреса кінцевого пристрою>

(для операційних систем Microsoft Windows)

або

traceroute <ім'я вузла призначення або адреса кінцевого пристрою>

(для Unix та Unix-подібних операційних систем)

Утиліти traceroute (або tracert) часто використовуються для пошуку та усунення несправностей в мережі. Переглядаючи перелік пройдених маршрутизаторів, можна визначити шлях, яким можна дістатися до певного місця призначення в мережі або через об'єднані мережі. Кожен маршрутизатор є точкою, в якій одна мережа з'єднується з іншою мережею і через нього пакет даних пересилається далі. Кількість маршрутизаторів, через які дані проходять від джерела до пункта призначення, відома як кількість хопів (hop - стрибок) .

Отриманий перелік може допомогти визначити проблеми під час передачі даних при спробі отримати доступ до сервісу, наприклад веб-сайту. Це також може бути корисним при виконанні таких завдань, як завантаження даних. Якщо один і той самий файл даних доступний для завантаження з декількох веб-сайтів (дзеркал), то можна відстежити шлях до кожного дзеркала, щоб вирішити, яке з них використати для найшвидшого отримання файлу.

Дві спроби відстежених маршрута між тими самими джерелом і пунктом призначення, які відрізняються в часі, можуть показати різні результати. Це пов'язано з "сітчастим" ("meshed") характером об'єднаних мереж, що передбачає здатність Інтернету та Інтернет-протоколів вибирати різні шляхи для надсилання пакетів.

Утиліти командного рядку для відстеження маршруту зазвичай вбудовуються до операційних систем кінцевих пристроїв.

Потрібно

Використовуючи підключення до Інтернету, ви спробуєте як працюють дві утиліти трасування маршруту для вивчення Інтернет шляху до мереж призначення. По-перше, ви перевірите чи є зв'язок із веб-сайтом. По-друге, ви будете використовувати утиліту traceroute у командному рядку Linux. По-третє, ви будете використовувати веб версію traceroute (http://www.monitis.com/traceroute/).

Послідовність виконання роботи

Перевірка доступності мережі за допомогою утиліти Ping

Запустіть CyberOps Workstation VM. Увійдіть до VM з наступними ідентифікаційними даними:

Ім'я користувача: **analyst**

Пароль: **cyberops**

Відкрийте вікно термінала у VM, щоб пропінгувати віддалений сервер, наприклад www.cisco.com .

[analyst@secOps ~]$ **ping -c 4 www.cisco.com**

PING e2867.dsca.akamaiedge.net (184.24.123.103) 56(84) bytes of data.

64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp_seq=1 ttl=59 time=13.0 ms

64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp_seq=2 ttl=59 time=12.5 ms

64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp_seq=3 ttl=59 time=14.9 ms

64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp_seq=4 ttl=59 time=11.9 ms

--- e2867.dsca.akamaiedge.net ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3005ms

rtt min/avg/max/mdev = 11.976/13.143/14.967/1.132 ms

Перший рядок відповіді показує повне доменне ім'я (FQDN) e2867.dsca.akamaiedge.net. Далі йде IP-адреса 184.24.123.103. Cisco тримає однаковий веб-контент на різних серверах по всьому світу (так званих дзеркалах). Тому, залежно від того, де ви знаходитесь географічно, FQDN та IP-адреса будуть різними.

Було надіслано чотири ехо-запити, і відповідь була отримана для кожного з них. Оскільки на кожен запит було отримано відповідь, зазначено, що було втрачено 0% пакетів. У середньому 3005 мс (3005 мілісекунд) часу знадобилося пакетам, щоб перетнути мережу. Мілісекунда - це $1/1000^{-на}$ секунди. Ваші результати скоріш за все будуть відрізнятися.

Перевірка доступності мережі за допомогою утиліти Traceroute

Тепер, коли доступність в цілому була підтверджена за допомогою утиліти ping, корисно поглянути більш докладно на кожен сегмент мережі, який перетинається.

Відстежені маршрути можуть проходити через безліч хопів і декілька інших провайдерів Інтернету (ISP) залежно від розміру вашого ISP та місця розташування хостів джерела та призначення. Кожен хоп представляє маршрутизатор. Маршрутизатор - це спеціалізований комп'ютер, який використовується для керування трафіком, який проходить через Інтернет. Уявіть собі, що подорожуєте автомобілем через кілька країн, використовуючи високошвидкісні шосе. У різні моменти подорожі ви проїжджаєте розвилку на дорозі, де можете обрати одну з декількох різних магістралей. А тепер далі уявіть, що на кожній розвилці дороги є пристрій,

який спрямовує вас на правильну магістраль до вашого кінцевого пункту призначення. Саме це робить маршрутизатор для пакетів у мережі.

Оскільки комп'ютери оперують двійковими або шістнадцятковими числами, а не словами, маршрутизатори однозначно ідентифікуються за допомогою IP-адрес. Утиліта **traceroute** показує, який шлях через мережу проходить пакет даних для досягнення цільового хоста. Також утиліта **traceroute** дає вам уявлення про те, наскільки швидко трафік передається в кожному сегменті мережі. Пакети надсилаються на кожен маршрутизатор, розташований на шляху, а час повернення вимірюється в мілісекундах.

Примітка: у параметрах мережі CyberOps Workstation VM, можливо, потрібно встановити режим моста, якщо ви не отримуєте жодних результатів traceroute. Щоб перевірити настройки мережі, перейдіть до: **Машина** > **Налаштування**, виберіть Мережа, вкладка Адаптер 1, Приєднується до: **Міст (Bridged Adapter)**.

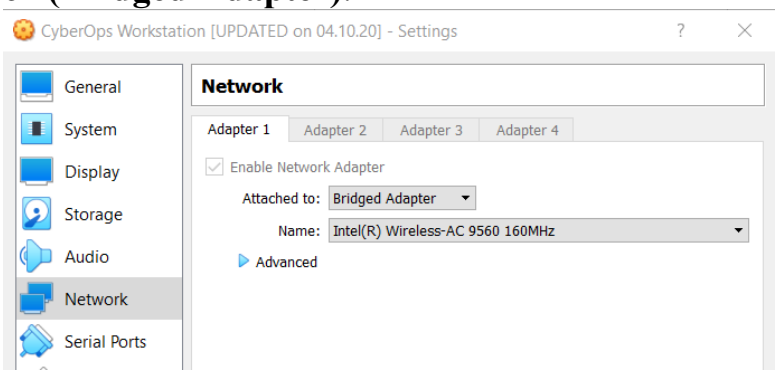

Рисунок 1 – Встановлення налаштувань CyberOps Workstation VM

Для цього використовується утиліта **}traceroute**.

У командному рядку термінала введіть **traceroute www.cisco.com**.

[analyst@secOps ~]$ **traceroute www.cisco.com**

traceroute to www.cisco.com (184.24.123.103), 30 hops max, 60 byte packets

1 192.168.1.1 (192.168.1.1) 6.527 ms 6.783 ms 6.826 ms

2 10.39.176.1 (10.39.176.1) 27.748 ms 27.533 ms 27.480 ms

3 100.127.65.250 (100.127.65.250) 27.864 ms 28.570 ms 28.566 ms

4 70.169.73.196 (70.169.73.196) 29.063 ms 35.025 ms 33.976 ms

5 fed1bbrj01.xe110.0.rd.sd.cox.net (68.1.0.155) 39.101 ms 39.120 ms 39.108 ms

6 a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103) 38.004 ms 13.583 ms 13.612 ms

Якщо ви хочете зберегти результат роботи traceroute до текстового файлу для подальшого перегляду, використовуйте символ > та бажане ім'я файлу, щоб зберегти результати у поточному каталозі. У цьому прикладі результат traceroute зберігається у файлі /home/analyst/cisco-traceroute.txt.

[analyst@secOps ~]$ **traceroute www.cisco.com > cisco-traceroute.txt**

Тепер ви можете ввести команду **cat cisco-traceroute.txt**, щоб переглянути результат трасування, збережений в текстовому файлі.

Виконайте та збережіть результати traceroute для одного з наступних веб-сайтів. Це веб-сайти регіональних інтернет-реєстраторів (RIR), які розташовані в різних частинах світу:

Африка: **www.afrinic.net**

Австралія: **www.apnic.net**

Європа: **www.ripe.net**

Південна Америка: **www.lacnic.net**

Примітка: Деякі з маршрутизаторів на маршруті можуть не відповідати на traceroute.

Відстеження маршруту до віддаленого сервера за допомогою веб-інструмента Traceroute

Відкрийте веб-браузер у віртуальній машини та знайдіть графічну версію traceroute, який можна використовувати у веб-браузері. Спробуйте перейти на наступний сайт: https://gsuite.tools/traceroute

Введіть будь-який сайт, який ви хочете. **Приклад: www.cisco.com** і натисніть « **Трасування**».

Примітка: Якщо у Firefox з'являється повідомлення про помилку «SEC_ERROR_OCSP_FUTURE_RESPOND», то на робочій станції CyberOps некоректно встановлений час. Щоб виправити час, введіть таку команду, щоб оновити годинник/час, та оновіть сторінку браузера і введіть візуальне трасування:

[analyst@secOps ~]$ **sudo ntpd -qg**

Ознайомтеся з географічним розташуванням хопів, які відповіли. Які коментарі ви можете зробити стосовно шляху?

Вимоги до звіту

Звіт по роботі повинен містити:

1. Назву дисципліни та лабораторної роботи.

2. Прізвище, ім’я та по батькові студента, код групи.

4. Знімки зображень екрану, які коментують виконання завдань.

5. Коментарі до кожного етапу.

5. Висновки.

Контрольні питання і завдання

1. Чим відрізняється traceroute на www.cisco.com або на інші веб-сайти з терміналу від веб-версії?

2. Як Ваші результати можуть відрізнятися залежно від того, де ви перебуваєте географічно, і який Інтернет-провайдер забезпечує підключення до Інтернету.

2.6 Лабораторна робота № 6
Використання Wireshark для спостереження за тристороннім рукостисканням TCP

Об'єкт: mininet топологія комп'ютерної мережі.

Мета: підготовка вузлів до захоплення трафіку. Проведення аналізу пакетів, використовуючи Wireshark. Перегляд пакетів за допомогою tcpdump.

Довідкова інформація

У цій лабораторії Ви будете використовувати Wireshark для захоплення і вивчення пакетів, що генеруються між браузером ПК за допомогою протоколу передачі гіпертексту (HTTP) і веб-сервера, наприклад www.google.com. Коли застосунок, наприклад HTTP або протокол передавання файлів (FTP) вперше запускається на хості, TCP використовує тристороннє рукостискання для встановлення надійного сеансу TCP між двома хостами. Наприклад, коли ПК використовує веб-браузер для серфінгу в Інтернеті, ініціюється тристороннє рукостискання і між хостом ПК і веб-сервером встановлюється сеанс. ПК може мати кілька одночасних, активних сеансів TCP з різними веб-сайтами.

Порядок виконання роботи

Підготовка вузлів до захоплення трафіку

Запустіть віртуальну машину CyberOps. Увійдіть, використовуючи ім'я користувача (username)**analyst** та пароль **cyberops**.

Start Mininet.

[analyst@secOps ~]$ **sudo lab.support.files/scripts/cyberops_topo.py**

Запустіть хост H1 і H4 в Mininet.

*** Starting CLI:

mininet> **xterm H1**

mininet> **xterm H4**

Запустіть веб-сервер на H4.

[root@secOps analyst]# **/home/analyst/lab.support.files/scripts/reg_server_start.sh**

З метою безпеки Ви не можете запустити Firefox використовуючи обліковий запис користувача root. На хості H1 використовуйте команду перемикання користувача, щоб перейти від користувача root до облікового запису користувача аналітика:

[root@secOps analyst]# **su analyst**

Запустіть веб-браузер на H1. Цей процес може зайняти декілька хвилин.

[analyst@secOps ~]$ **firefox &**

Після того, як відкриється вікно Firefox, запустіть сесію tcpdump в **терміналі Node: H1** і відправте висновок в файл під назвою **apture.pcap**. За допомогою опції -v Ви можете спостерігати за прогресом. Цей захоплення зупиниться після захоплення 50 пакетів, оскільки він налаштований з опцією -c 50.

[analyst@secOps ~]$ **sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap**

Після запуску tcpdump швидко перейдіть до 172.16.0.40 в веб-браузері Firefox.

Analyze the Packets using Wireshark

Застосуйте фільтр до збереженого знімка.

Натисніть Enter щоб побачити командний рядок. Запустіть Wireshark на**вузлі: H1**. Натисніть кнопку **OK** , коли з'явиться попередження про запуск Wireshark від імені суперкористувача.

[analyst@secOps ~]$ **wireshark &**

У Wireshark послідовно виберіть елементи **Файл** > **Відкрити**. Виберіть збережений файл pcap, розташований за адресою /home/analyst/capture.pcap.

Застосуйте фільтр**tcp** до збереженого знімка. У цьому прикладі перші 3 кадри, це той трафік, що нас цікавить.

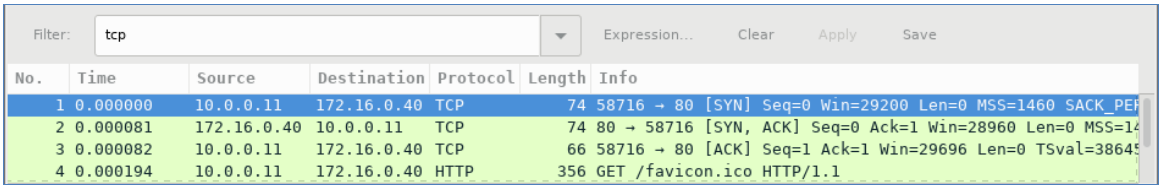

Рисунок 2 – Застосування фільтрів

Перегляньте інформацію в пакетах, включаючи IP-адреси, номери TCP-портів і позначки керування TCP.

У цьому прикладі кадр 1 — це початок тристороннього рукостискання між ПК і сервером на H4. В області списку пакетів (верхній розділ головного вікна) виберіть перший пакет, якщо це необхідно.

Натисніть **стрілку** ліворуч від Протоколу керування передачею в області відомостей пакета, щоб розгорнути його та вивчити відомості про TCP. Знайдіть інформацію про порт джерела та призначення.

Натисніть **стрілку** зліва від прапорця. Значення 1 означає, що встановлено прапорець. Знайдіть прапорець, який встановлено в цьому пакеті.

Примітка. Можливо, Вам доведеться налаштувати розміри верхнього та середнього вікон у Wireshark, щоб відобразити необхідну інформацію.

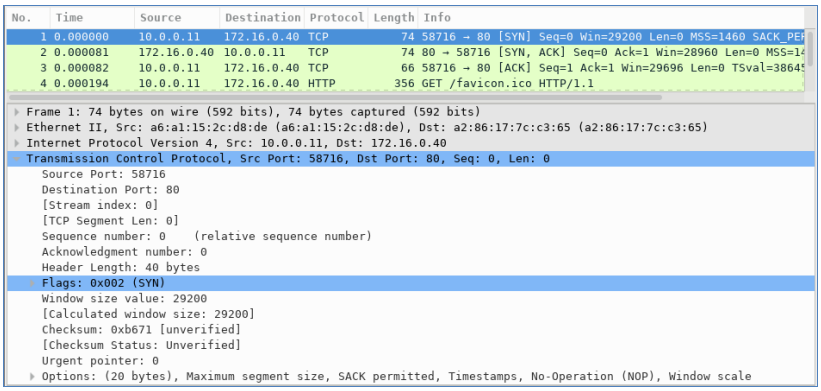

Рисунок 3 – Налаштування розмірів вікон

Що таке номер порту джерела TCP?

Як би Ви класифікували вихідний порт?

Який номер порту призначення TCP?

Як би Ви класифікували порт призначення?

Який прапорець (або прапорці) встановлений?

Що таке відносний порядковий номер?

Виберіть наступний пакет в тристоронньому рукостисканні. У цьому прикладі це кадр 2. Це веб-сервер, який дає відповідь на початковий запит на початку сеансу.

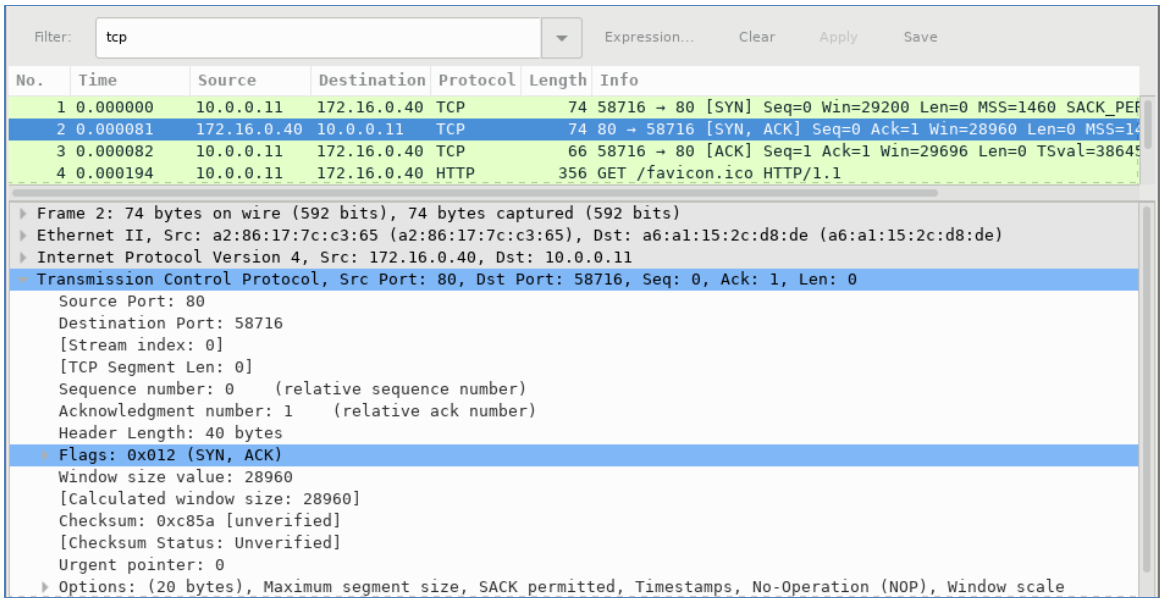

Рисунок 4 – Вибір пакетів для аналізу

Які порти джерела та призначення?

Які прапорці встановлені?

Які відносні порядкові номери та номери підтвердження?

Нарешті, виберіть третій пакет в тристороннім рукостисканням.

Перегляньте третій і останній пакет рукостискання.

Який прапорець (або прапорці) встановлений?

Відносні порядкові номери та номери підтвердження встановлюються рівними 1, як початова точка. Підключення TCP встановлено і може початися зв'язок між вихідним комп'ютером і веб-сервером.

Перегляньте пакети за допомогою tcpdump.

Також можна переглянути файл pcap і відфільтрувати потрібну інформацію.

Відкрийте нове вікно термінала, введіть **man tcpdump**. **Примітка.**: Можливо, знадобиться натиснути клавішу ENTER, щоб переглянути запит.

Використовуючи сторінки довідника доступні в операційній системі Linux, Ви читаєте або шукаєте на сторінках посібника варіанти вибору потрібної інформації з файлу pcap.

[analyst@secOps ~]$ **man tcpdump**

TCPDUMP(1) General Commands Manual TCPDUMP(1)

NAME

tcpdump - dump traffic on a network

SYNOPSIS

tcpdump [-AbdDefhHIJKlLnNOpqStuUvxX#] [-B buffer_size]
[-c count]
[-C file_size] [-G rotate_seconds] [-F file]
[-i interface] [-j tstamp_type] [-m module] [-M secret]
[--number] [-Q in|out|inout]
[-r file] [-V file] [-s snaplen] [-T type] [-w file]
[-W filecount]
[-E spi@ipaddr algo:secret,...]
[-y datalinktype] [-z postrotate-command] [-Z user]
[--time-stamp-precision=tstamp_precision]
[--immediate-mode] [--version]
[expression]

<some output omitted>

Для пошуку по сторінках man Ви можете використовувати/(пошук вперед) або? (пошук назад), щоб знайти конкретні терміни, і **n** перейти до наступного збігу і **q**, щоб вийти. Наприклад, шукаємо інформацію на перемикачі -r, набираємо **/-r**. Натисніть **n** , щоб перейти до наступного збігу.

Що робить перемикач **-r** ?

У цьому ж терміналі відкрийте файл захоплення за допомогою наступної команди, щоб переглянути перші 3 захоплених TCP пакетів:

[analyst@secOps ~]$ **tcpdump -r /home/analyst/capture.pcap tcp -c 3**

reading from file capture.pcap, link-type EN10MB (Ethernet)

13:58:30.647462 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [S], seq 2432755549, win 29200, options [mss 1460,sackOK,TS val 3864513189 ecr 0,nop,wscale 9], length 0

13:58:30.647543 IP 172.16.0.40.http > 10.0.0.11.58716: Flags [S.], seq 1766419191, ack 2432755550, win 28960, options [mss 1460,sackOK,TS val 50557410 ecr 3864513189,nop,wscale 9], length 0

13:58:30.647544 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 3864513189 ecr 50557410], length 0

Для перегляду тристороннього рукостискання може знадобитися збільшити кількість рядків після параметра **-c**.

Перейдіть на термінал, який використовується для запуску Mininet. Завершіть роботу Mininet, увівши quit у головному вікні терміналу CyberOps VM

mininet> **quit**
*** Stopping 0 controllers

*** Stopping 2 terms
*** Stopping 5 links
.....
*** Stopping 1 switches
s1
*** Stopping 5 hosts
H1 H2 H3 H4 R1
*** Done
[analyst@secOps ~]$

Після завершення роботи з Mininet, натисніть enter **sudo mn -c**, щоб очистити процеси, започатковані Mininet. Введіть пароль **cyberops** коли з'явиться підказка.

[analyst@secOps ~]$ **sudo mn -c**
[sudo] password for analyst:

Вимоги до звіту

Звіт по роботі повинен містити:

1. Назву дисципліни та лабораторної роботи.
2. Прізвище, ім’я та по батькові студента, код групи.
4. Знімки зображень екрану, які коментують виконання завдань.
5. Коментарі до кожного етапу.
5. Висновки.

Контрольні питання і завдання

1. Дати відповіді на питання кожного етапу роботи.
2. У Wireshark доступні сотні фільтрів. Велика мережа може мати численні фільтри та багато різних типів трафіку. Перелічіть три фільтри, які можуть бути корисними адміністратору мережі?
3. Як ще можна використовувати Wireshark у виробничій мережі?

2.7 Лабораторна робота № 7
Використання Wireshark для дослідження HTTP та HTTPS трафіку

Об'єкт: HTTP та HTTPS трафік.

Мета: захоплення та перегляд трафіку HTTP. Захоплення та перегляд трафіку HTTPS.

Довідкова інформація

Протокол передавання гіпертекстових повідомлень (HTTP) - це протокол прикладного рівня, який представляє дані через веб-браузер. HTTP не забезпечує захисту даних, якими обмінюються два взаємодіючі пристрої.

В HTTPS для шифрування використовується математичний алгоритм. Цей алгоритм приховує справжній зміст даних, якими обмінюється. Це робиться за допомогою сертифікатів, які можна переглянути пізніше в цій лабораторній роботі.

Незалежно від HTTP або HTTPS, рекомендується обмінюватися даними лише з веб-сайтами, яким ви довіряєте. Той факт, що сайт використовує HTTPS, не означає, що він надійний. Зловмисники зазвичай використовують HTTPS, щоб приховати свою діяльність.

У цій лабораторній роботі ви будете досліджувати і захоплювати HTTP і HTTPS трафік за допомогою Wireshark.

Порядок виконання роботи

Захоплення та перегляд трафіку HTTP

У цій частині ви будете використовувати **tcpdump** для захоплення вмісту HTTP-трафіку. Ви будете використовувати параметри команд для збереження трафіку в файл захоплення пакетів (pcap). Ці записи потім можна проаналізувати за допомогою різних додатків, які читають файли pcap, включаючи Wireshark.

Запустіть віртуальну машину та увійдіть до системи

Запустіть CyberOps Workstation VM. Використовуйте такі облікові дані користувача:

Ім'я користувача: **analyst**

Пароль: **cyberops**

Відкрийте термінал і запустіть tcpdump.

Відкрийте застосунок терміналу і введіть команду**ip address**.

[analyst@secOps ~]$ **ip address**

Перелічить інтерфейси і їх IP-адреси, що відображаються у вихідних даних команди **ip address**.

Перебуваючи в застосунку терміналу, введіть команду **sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap**. Коли буде запропоновано, введіть пароль **cyberops** для користувача analyst.

[analyst@secOps ~]$ **sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap**

[sudo] password for analyst:

tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

Ця команда запускає tcpdump і записує мережевий трафік на інтерфейсі **enp0s3**.

Параметр **-i** для команди дозволяє вказати інтерфейс. Якщо параметр не вказано, tcpdump буде захоплювати весь трафік на всіх інтерфейсах.

Параметр команди **-s** визначає довжину знімка для кожного пакета. Ви повинні обмежити snaplen найменшим числом, яке буде захоплювати інформацію про протокол, яка вас цікавить. Встановлення snaplen на 0 встановлює значення за замовчуванням 262144 для зворотної сумісності з останніми старими версіями tcpdump.

Параметр команди **-w** використовується для запису результату команди tcpdump в файл. Додавання розширення .pcap гарантує, що операційні системи та програми зможуть читати файл. Весь записаний трафік буде роздрукований в файл httpdump.pcap в домашньому каталозі користувача analytics.

Використовуйте сторінки довідки для tcpdump, щоб визначити використання параметрів команди -s і -w.

Відкрийте веб-браузер з панелі запуску в VM робочої станції CyberOps. Перейдіть до **http://www.altoromutual.com/login.jsp**

Оскільки цей веб-сайт використовує HTTP, трафік не шифрується. Клацніть на поле Пароль (Password), щоб побачити спливаюче попередження.

Введіть ім'я користувача **Admin** з паролем **Admin** і натисніть **Login (Увійти)**.

Закрийте веб-браузер.

Поверніться до вікна терміналу, де запущено tcpdump. Введіть **CTRL+C** , щоб зупинити захоплення пакетів.

Перегляньте захоплення HTTP.

Tcpdump, виконаний на попередньому кроці, записав вихідні дані у файл з ім'ям httpdump.pcap. Цей файл знаходиться в домашньому каталозі користувача **analyst**.

Клацніть на піктограмі File Manager (Диспетчер файлів) на робочому столі та перейдіть до домашнього каталогу користувача **analyst**. Двічі клацніть на файлі **httpdump.pcap**, у діалоговому вікні Open With (Відкрити за допомогою) прокрутіть вниз до Wireshark і натисніть кнопку **Open (Відкрити)**.

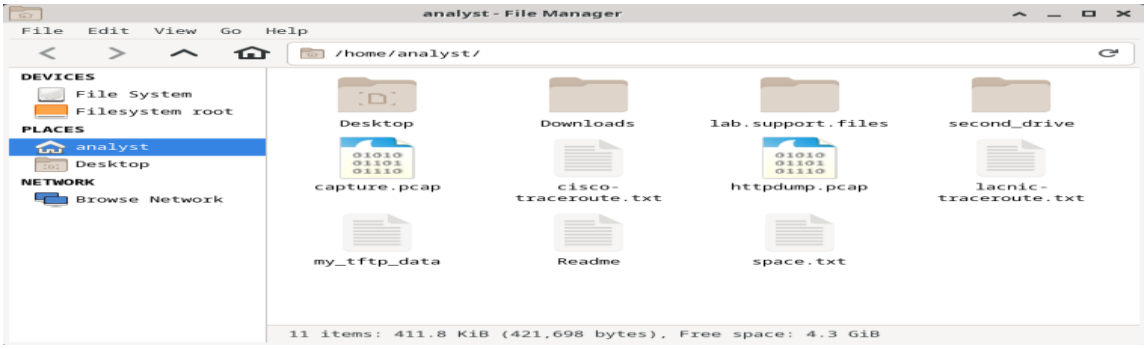

Рисунок 1 – Відкриття пакету Wireshark

У застосунку Wireshark відфільтруйте **http** і натисніть **Apply (Застосувати)**.

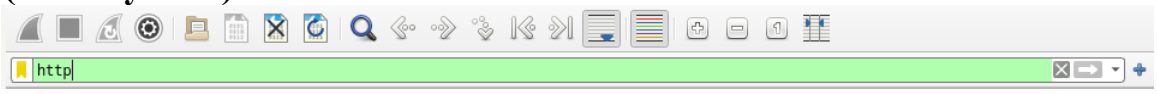

Рисунок 2 – Фільтрація HTTP-повідомлень.

Перегляньте різні HTTP-повідомлення та виберіть повідомлення **POST**.

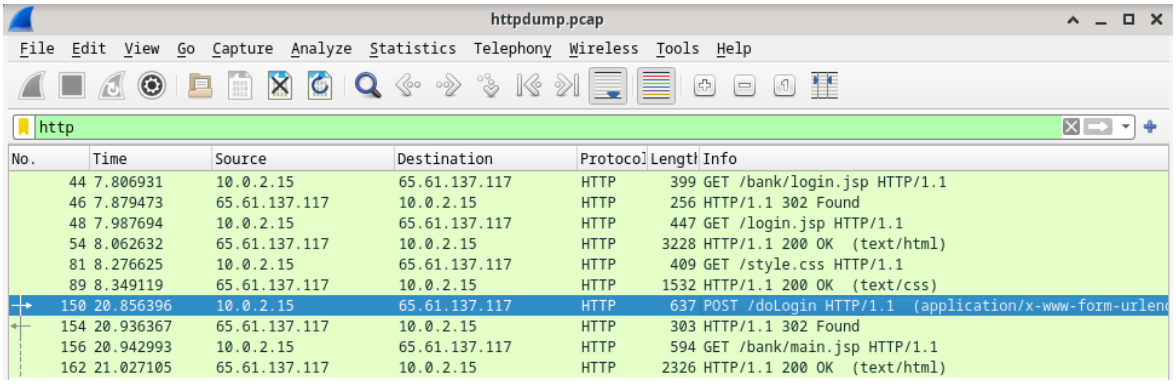

Рисунок 3 – Перегляд інформації про HTTP-повідомлення.

У нижньому вікні відображаються повідомлення. Розгорніть розділ **HTML Form URL Encoded: application/x-www-form-urlencoded**.

Які два фрагменти інформації відображаються?

Закрийте програму Wireshark.

Захоплення та перегляд трафіку HTTPS

Тепер ви використовуватимете tcpdump із командного рядка робочої станції Linux для захоплення трафіку HTTPS. Після запуску tcpdump ви будете генерувати трафік HTTPS, а tcpdump записуватиме вміст мережевого трафіку. Ці записи знову буде проаналізовано за допомогою Wireshark.

Запустіть tcpdump у терміналі.

Перебуваючи в застосунку терміналу, введіть команду **sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap**. Коли буде запропоновано, введіть пароль **cyberops** для користувача analyst.

[analyst@secOps ~]$ **sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap**

[sudo] password for analyst:

tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

Ця команда запускає tcpdump і записує мережевий трафік на інтерфейсі **enp0s3** робочої станції Linux. Якщо ваш інтерфейс відрізняється від enp0s3, будь ласка, змініть його при використанні вищевказаної команди.

Весь записаний трафік буде занесено в файл **httpsdump.pcap** в домашньому каталозі користувача analyst.

Відкрийте веб-браузер з панелі запуску в VM робочої станції CyberOps. Перейдіть на сторінку www.netacad.com.

Примітка: Якщо ви отримали веб-сторінку «Secure Connection Failed (Помилка безпечного з’єднання)», ймовірно, це означає, що дата й час неправильні. Оновіть день і час за допомогою такої команди, змінивши поточний день і час:

[analyst@secOps ~]$ **sudo date -s "12 MAY 2020 21:38:20**

Що ви помітили в URL-адресі веб-сайту?

Натисніть **Log in (Увійти)**.

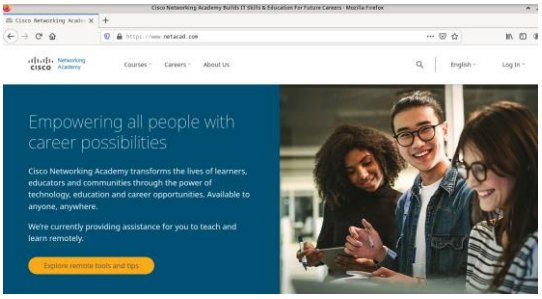

Рисунок 4 – Початкова сторінка NetaCAD

Введіть свої ім'я користувача та пароль для NetaCAD. Натисніть **Next (Далі)**.

Закрийте веб-браузер у віртуальній машині.

Поверніться до вікна терміналу, де запущено tcpdump. Введіть **CTRL+C** , щоб зупинити захоплення пакетів.

Перегляньте захоплення HTTPS.

Tcpdump, виконаний на кроці 1, записав вихідні дані до файлу з назвою httpsdump.pcap. Цей файл знаходиться в домашньому каталозі користувача **analyst**.

Клацніть на піктограму Filesystem (Файлова система) на робочому столі та перейдіть до домашнього каталогу для користувача analyst. Відкрийте файл **httpsdump.pcap**.

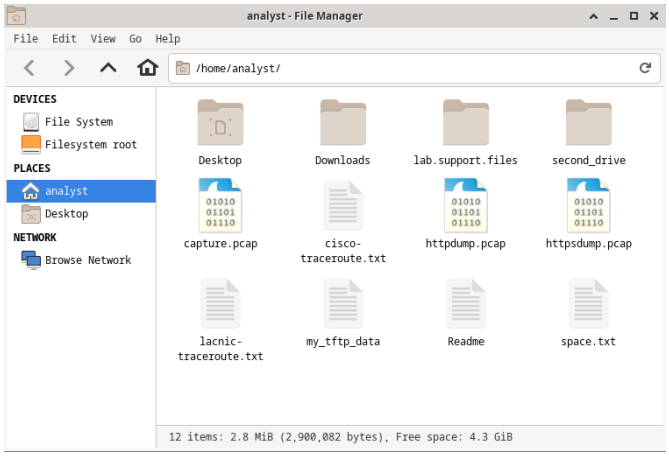

Рисунок 5 – Використання менеджеру файлів

У програмі Wireshark розгорніть вікно захоплення по вертикалі, а потім відфільтруйте трафік HTTPS через порт 443.

Введіть **tcp.port==443** як фільтр і натисніть кнопку **Apply (Застосувати)**.

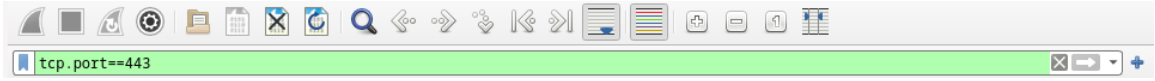

Рисунок 6 - Відфільтрування трафіку HTTPS через порт 443

Перегляньте різні повідомлення HTTPS і виберіть повідомлення **Application Data (Дані програми)**.

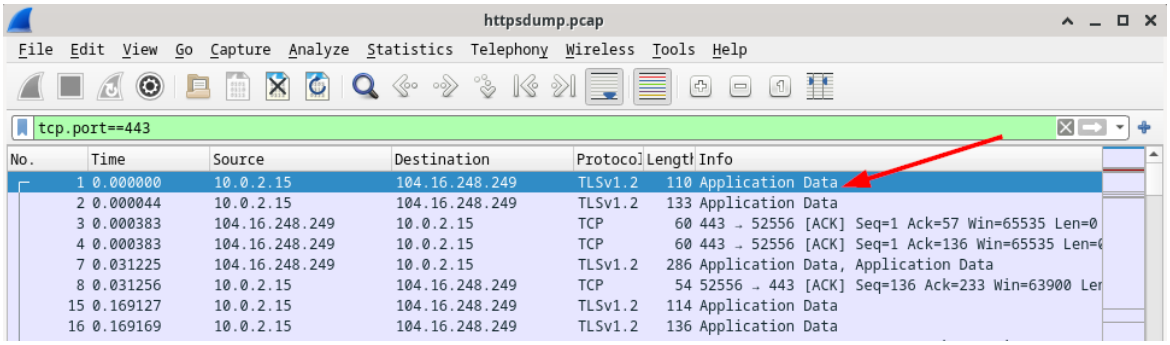

Рисунок 7 – Перегляд повідомлень трафіку HTTPS через порт 443

У нижньому вікні відображаються повідомлення.

Що замінило розділ HTTP, який був у попередньому файлі захоплення?

Повністю розгорніть розділ **Secure Sockets Layer**.

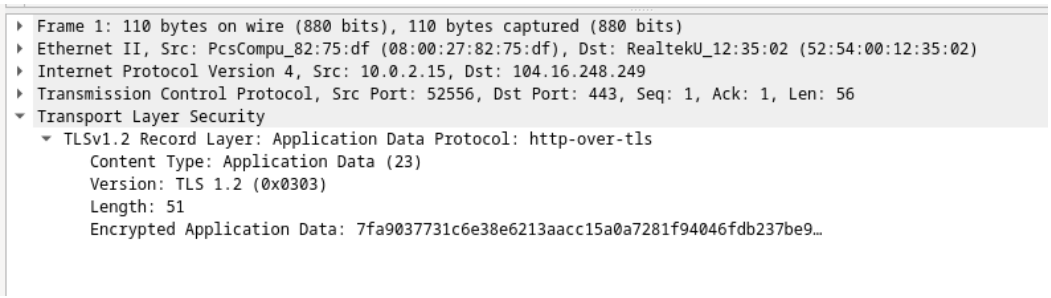

Рисунок 8 – Характеристика повідомлень трафіку

Натисніть кнопку **Encrypted Application Data (Зашифровані дані програми)**.

Чи є дані програми у відкритому текстовому чи читабельному форматі?

Закрийте всі вікна і вимкніть віртуальну машину.

Питання для самоперевірки

Які переваги використання HTTPS замість HTTP?

Чи всі веб-сайти, які використовують HTTPS, вважаються надійними?

Вимоги до звіту

Звіт по роботі повинен містити:

1. Назву дисципліни та лабораторної роботи.
2. Прізвище, ім’я та по батькові студента, код групи.
4. Знімки зображень екрану, які коментують виконання завдань.
5. Коментарі до кожного етапу.
5. Висновки.

Контрольні питання і завдання

1. Дати відповіді на питання кожного етапу роботи.
2. Які переваги використання HTTPS замість HTTP?
3. Чи всі веб-сайти, які використовують HTTPS, вважаються надійними?

3. **КРИТЕРІЇ ОЦІНЮВАННЯ**

Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90–100	відмінно
74–89	добре
60–73	задовільно
0–59	незадовільно

Здобувачі можуть отримати підсумкову оцінку з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів складатиме не менше як 60 балів.

Максимальне оцінювання становить:

Теоретична частина	Лабораторні роботи	**Разом**
51	49	**100**

Критерії оцінювання лабораторної роботи

За кожну лабораторну роботу здобувач може отримати до 7 балів (усього 49 бали), а саме:

7 балів: звіт з роботи оформлений згідно з методичними рекомендаціями і містить повні, інформативні та обґрунтовані висновки.

5 бали: звіт з роботи оформлений із незначними відхиленнями від методичних рекомендацій або висновки не повністю задовольняють вимогам повноти, інформативності та обґрунтованості.

3 бали: звіт з роботи оформлений із суттєвими відхиленнями від методичних рекомендацій, або висновки не задовольняють вимогам повноти, інформативності та обґрунтованості.

0 балів: звіт з роботи відсутній, або не містить висновків, або висновки протирічать фактично отриманим результатам.

У разі отримання позитивної оцінки студент може підвищити її шляхом очної співбесіди з викладачем. При цьому за кожну правильну відповідь на запропоновані запитання нараховується 1 бал.

СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Захист інформації в комп'ютерних системах та мережах: навч. посіб. / С.Г. Семенов, А.О. Подорожняк, О.І. Баленко, С.Ю. Гавриленко. – Харків : НТУ «ХПІ», 2014.– 251 с.
2. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологія і мережах [Електронний ресурс] : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології» / В.П. Полторак. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 78 с.
3. Платформа дистанційної освіти мережної академії Cisco. Навчальний курс «Big Data & Analytics». [URL: **https://www.netacad.com/courses/cybersecurity/ccna-security**]
4. Kizza J. M. Guide to Computer Network Security Springer. Series Title: Computer Communications and Networks, London 2015, 545 p. https://doi.org/10.1007/978-1-4471-6654-2
5. Miller, A. R. The Cryptographic Mathematics of Enigma, Center for Cryptologic History National Security Agency [Електронний ресурс] / A. R. Miller // Google Диск. – 2019. – Режим доступу: https://drive.google.com/file/d/1By1nea1BhIiNwCfykdmQAawkyh5QT_hr/view. – Дата доступа: 20.02.2020.
6. Soni, A., Upadhyay, R., Jain, A. (2017). Internet of Things and Wireless Physical Layer Security: A Survey. In: Satapathy, S., Bhateja, V., Raju, K., Janakiramaiah, B. (eds) Computer Communication, Networking and Internet Security. Lecture Notes in Networks and Systems, vol 5. Springer, Singapore. **https://doi.org/10.1007/978-981-10-3226-4_11**
7. Shivanna, K., Deva, S.P., Santoshkumar, M.. Privacy Preservation in Cloud Computing with Double Encryption Method. In: Satapathy, S., Bhateja, V., Raju, K., Janakiramaiah, B. (eds) Computer Communication, Networking and Internet Security. Lecture Notes in Networks and Systems, vol 5. Springer, Singapore, (2017) **https://doi.org/10.1007/978-981-10-3226-4_12**

ЗМІСТ

Навчальне видання

Дереза Андрій Юрійович
Шедловська Яна Ігорівна
Шедловський Ігор Анатолійович

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня магістра
галузі знань F Інформаційні технології

Видано в авторській редакції

Електронний ресурс.
Підписано до видання 19.05.2025. Авт. арк. 4,0.

Національний технічний університет «Дніпровська політехніка».
49005, м. Дніпро, просп. Дмитра Яворницького, 19.