МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з курсу

"Основи кібербезпеки"

для студентів спеціальність

«Кібербезпека»

ТЕРНОПІЛЬ – 2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з курсу

"Основи кібербезпеки"

для студентів спеціальність

«Кібербезпека»

ТЕРНОПІЛЬ – 2018

Методичні вказівки до виконання лабораторних робіт з курсу "Основи кібербезпеки" для студентів спеціальностей "Кібербезпека" / Укл.: Яцків В. В. – Тернопіль: Економічна думка, 2018. – 44 с.

Відповідальний за випуск: Яцків В.В. д.т.н., доцент,
завідувач кафедри кібербезпеки

Рецензенти: к.т.н., доцент Шевчук Р.П.
к.т.н., доцент Якименко І.З.

Методичні вказівки розглянуті та схвалені на засіданні кафедри кібербезпеки, протокол №2 від 27 вересня 2018 р.

Методичні вказівки затверджені на засіданні науково- методичної комісії з кібербезпеки, протокол № 4 від 27 вересня 2018 р.

ЗМІСТ

Вступ

Дисципліна “Основи кібербезпеки” є однією з перших і базових в системі знань і вмінь, що формують бакалавра за спеціальністю “Кібербезпека”.

Метою викладення дисципліни “Основи кібербезпеки” є: дізнатися, як захищатись в Інтернеті; ознайомитись з різними типами шкідливих програм і атак та методами захисту організацій від них; дізнатись про можливі варіанти кар'єри в галузі кібербезпеки. До кінця цього курсу студенти будуть більше обізнані щодо важливості безпечної поведінки в Інтернеті, можливих наслідків кібератак та можливих варіантів кар'єри в кібербезпеці.

Вивчення дисципліни “Основи кібербезпеки” дає студентам необхідну теоретичну і практичну підготовку для того, щоб вміти аналізувати наслідки кібератаки; знати різні категорії вразливостей програмного та апаратного забезпечення та систем безпеки; знати різні типи зловмисного ПЗ (відомого як шкідливі програми) та їх симптоми; знати різні методи, якими нападники можуть проникнути в систему: соціальна інженерія, злам паролю Wi-Fi, фішинг та використання вразливостей.

Виконання студентами лабораторних робіт з курсу “Основи кібербезпеки” дозволяє закріпити теоретичні знання і практичні навики.

Лабораторна робота №1

Перевірка цілісності даних

Мета роботи: вивчення програм хешування для перевірки цілісності даних

Необхідні ресурси.

• ПК з доступом до Інтернету

1. Теоретичні відомості

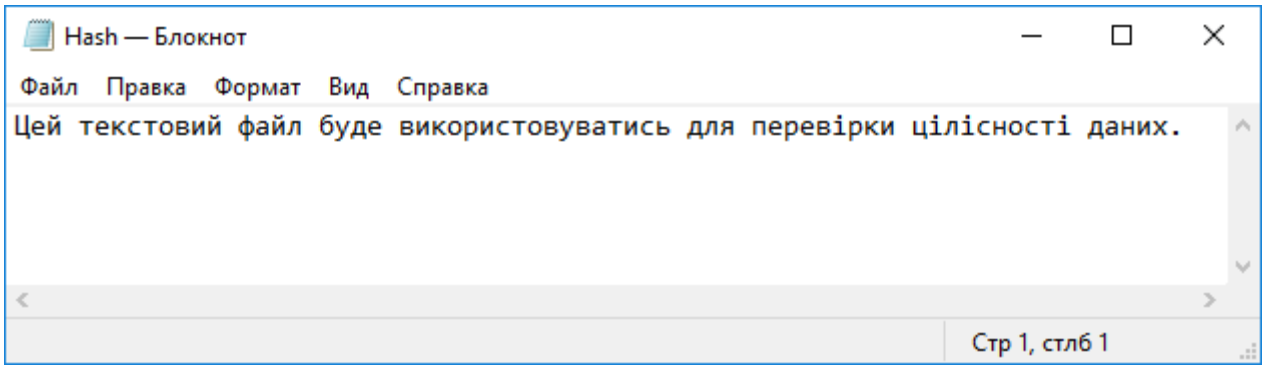
Важливо зрозуміти, що дані були пошкоджені або підмінені. Програма хешування може бути використана для перевірки - змінилися дані, чи вони залишилися незмінними. Програма хешування обчислює хеш-функцію з даних або файлу, та повертає значення (як правило, набагато коротше). Є багато різних хеш-функцій, деякі дуже прості, а деякі дуже складні. Коли однакова хеш-функція виконується з однаковими даними, то значення, що повертається, завжди однакове. Якщо з даними відбуваються будь-які зміни, то повернене значення хешу буде іншим.

2. Порядок виконання роботи

2.1. Створіть текстовий файл.

a. Знайдіть на своєму комп'ютері програму Блокнот (Notepad) і відкрийте її.

b. Введіть текст у програмі.



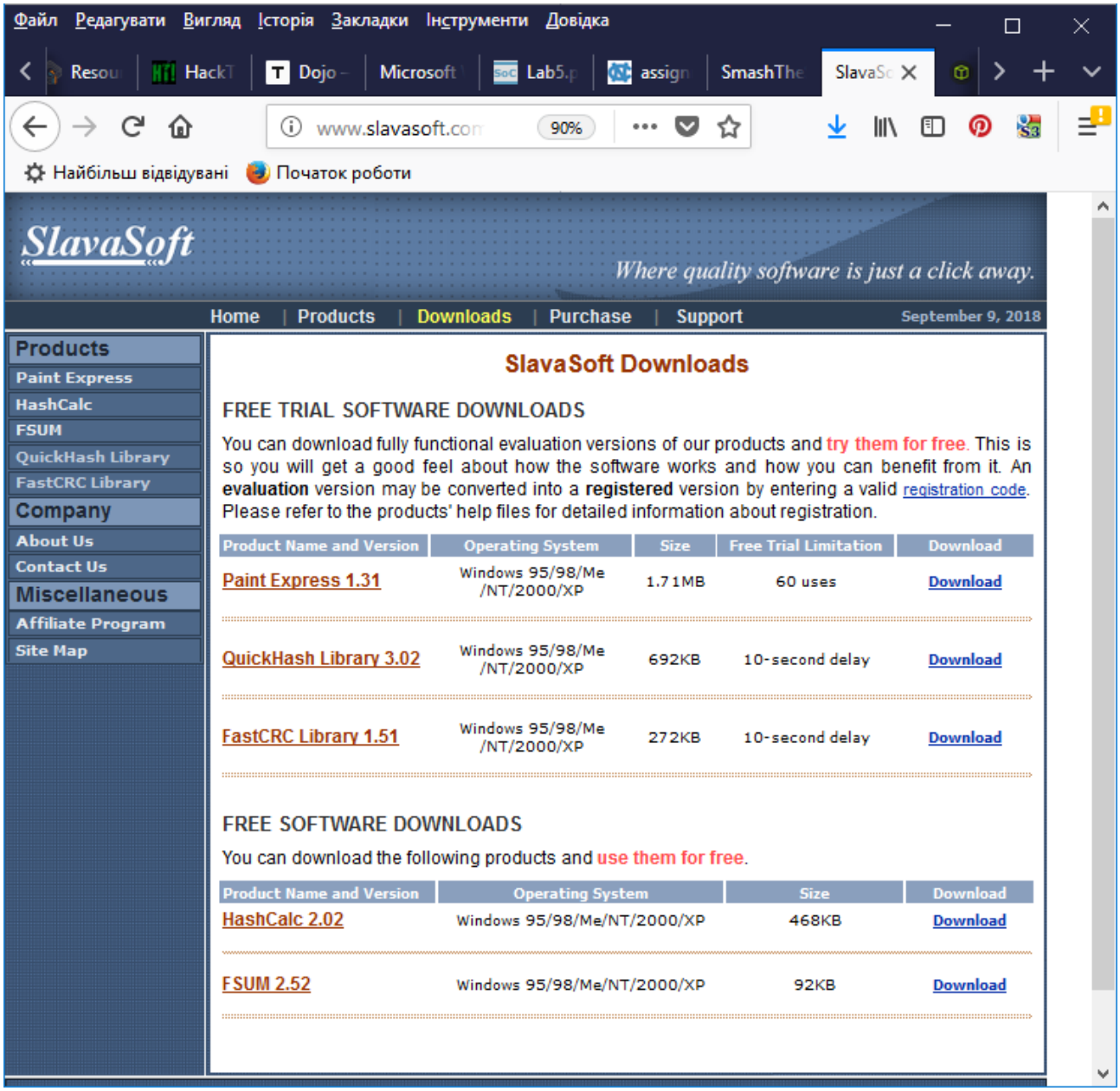
c. Виберіть **Файл > Зберегти (File > Save)**.

d. Перейдіть до **Робочого столу**

e. Введіть **Hash** у поле **Ім'я файлу: (File name:)** і натисніть **Зберегти (Save)**.

2.2 Встановіть HashCalc

a. Відкрийте веб-браузер і перейдіть за посиланням http://www.slavasoft.com/download.htm.



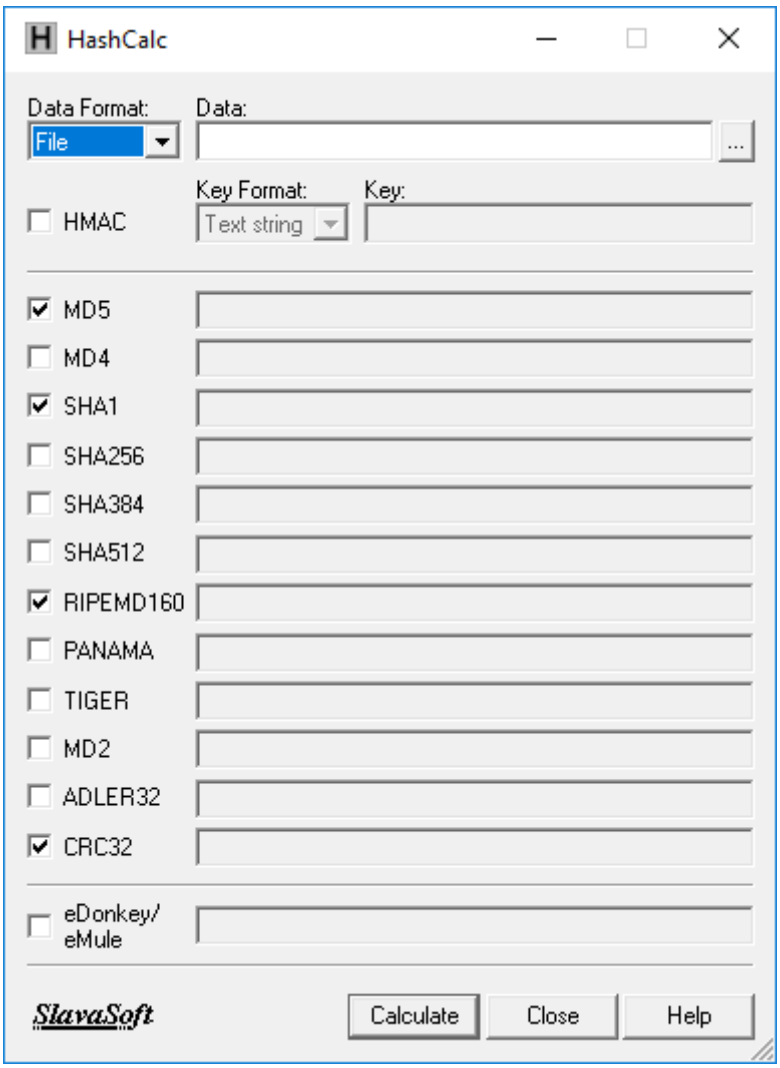
b. Натисніть **Завантажити (Download)** у рядку **HashCalc**.

c. Відкрийте **hashcalc.zip** файл та запустіть файл **setup.exe**.

d. Дотримуйтесь вказівок Майстра установки (Installation wizard), щоб встановити HashCalc. Попросіть у викладача допомогти, якщо у вас є будь-які питання про встановлення програми.

e. Натисніть кнопку **Готово (Finish)** на останньому екрані та закрийте файл **README**, якщо він відкритий. Ви можете прочитати файл, якщо хочете.

f. HashCalc тепер встановлено та запущено.



2.3. Обчисліть хеш файлу Hash.txt

a. Вкажіть наступні елементи у HashCalc:

1) Формат даних (Data Format): **Файл (File)**.

2) Дані: Натисніть **...** Поруч із полем **Дані** (Data), перейдіть на **Робочий стіл (Desktop)**і виберіть файл **Hash.txt**.

3) Зніміть прапорець **HMAC**

4) Зніміть усі типи хешів, крім **MD5**

b. Натисніть кнопку **Обчислити (Calculate)**.

Яке значення поряд із **MD5**?.

2.4. Внесіть зміни у файлі Hash.txt

c. Перейдіть на **Робочий стіл** і відкрийте файл **Hash.txt**.

d. Зробіть невелику зміну тексту, наприклад, видалення літери або додавання пробілу.

e. Натисніть **Файл > Зберегти (File > Save)** та закрийте **Блокнот**.

2.5. Обчисліть новий хеш файлу **Hash.txt**

a. Знову натисніть кнопку **Обчислити (Calculate)** в HashCalc.

Яке значення поряд із **MD5**?.

Чи значення відрізняється від значення, що одержано на кроці 3?

b. Встановіть прапорець біля усіх типів хеш-функцій.

c. Натисніть **Обчислити (Calculate)**

d. Зверніть увагу, що багато типів хеш-функцій створюють хеш різної довжини.

Поясніть чому?

Онлайн калькулятори для обчислення хеш – функцій:
https://www.fileformat.info/tool/hash.htm
https://www.tools4noobs.com/online_tools/hash/
http://foxtools.ru/Hash

3. Зміст звіту

3.1. Тема і мета роботи.
3.2. Вихідні дані для виконання роботи.
3.3. Результати виконання роботи
3.4. Висновки

Контрольні запитання

1. Для чого призначена хеш – функція?
2. Назвіть основні алгоритми обчислення хеш – функцій?
3. Як змінюється довжина хеш – функції при зміні вхідних даних?
4. Чи можна відновити дані, коли відома хеш – функція?

Лабораторна робота №2

Створення та збереження надійних паролів

Мета роботи: зрозуміти концепцію надійного пароля.

Дослідження концепцій створення надійного пароля.

Необхідні ресурси

• ПК або мобільний пристрій з доступом до Інтернету

1. Теоретичні відомості

Паролі широко використовуються для захисту доступу до ресурсів. Зловмисники можуть використовувати багато методів для розкриття паролів користувачів та отримання несанкціонованого доступу до ресурсів або даних.

Щоб краще захистити себе, важливо розуміти, що робить пароль надійним і як його безпечно зберігати.

Створення надійного пароля. Надійні паролі мають відповідати вимогам, які перелічені в порядку важливості:

1. Користувач може легко запам'ятати пароль.

2. Для будь-якої іншої людини вгадати цей пароль не є тривіальною задачею.

3. Вгадати або розкрити цей пароль не є тривіальною задачею для програми.

4. Пароль має бути складним, містити цифри, символи та суміш літер у верхньому та нижньому регістрах.

Виходячи з вищезазначеного переліку, перша вимога, мабуть, є найважливішою, оскільки вам потрібно ваш пароль пам'ятати. Наприклад, пароль **#4ssFrX^-aartPOknx25_70!xAdk<d!** вважається надійним, оскільки він задовольняє останнім трьом вимогам, але його буде дуже важко запам'ятати.

Багато організацій вимагають, щоб паролі містили комбінацію цифр, символів та літер у нижньому та верхньому регістрах. Паролі, які відповідають цій політиці, вважаються задовільними, якщо вони легко запам'ятовуються.

Нижче наведено приклад політики щодо вибору пароля для типової організації:

Довжина пароля має бути мінімум 8 символів.

Пароль повинен містити символи у верхньому і нижньому регістрах.

Пароль має містити хоча б одну цифру.

Пароль має містити хоча б один неалфавітний символ.

Проаналізуйте характеристики надійного пароля та загальну політику вибору паролів, наведену вище.

Чому в політиці не враховуються перші два пункти? Поясніть.

Гарною практикою створення надійних паролів є вибір чотирьох або більше випадкових слів і їх поєднання. Пароль **televisionfrogbootschurch** надійніший ніж **J0n@than#81**. Зверніть увагу, що, хоча другий пароль відповідає описаним вище правилам, програми зламу паролів дуже ефективні при визначенні цього типу пароля. Хоча багато політик створення паролів не дозволять використання першого пароля, **televisionfrogbootschurch**, він набагато надійніший ніж другий. Користувачу простіше його запам'ятати (особливо якщо він асоціюється з зображенням), він дуже довгий і фактор випадковості ускладнює визначення такого пароля.

Використовуючи онлайн-інструмент для створення паролів, створіть паролі на основі загальної політики компанії щодо створення паролів, яка була описана вище.

Типи атак на пароль.

1) Вгадування паролю. Найпоширеніший тип атаки — вгадування пароля. Зломщики можуть вгадувати паролі локально або дистанційно, вручну і з застосуванням автоматичних методів. Іноді вгадати пароль простіше, ніж здається на перший погляд. У налаштуваннях більшості мереж не потрібні довгі і складні паролі, і зломщикові достатньо знайти лише один слабкий пароль, щоб отримати доступ до мережі. Не всі протоколи аутентифікації однаково ефективні проти спроб угадування паролів. Наприклад, процедура аутентифікації LAN Manager нечутлива до регістра символів, тому при відгадуванні пароля не доводиться враховувати регістр букв.

Багато знарядь злому автоматизують процес, вводячи пароль за паролем. Деякі широко поширені інструменти відгадування: Hydra для відгадування будь-яких паролів, в тому числі HTTP, Telnet і Windows; TSGrinder для атак методом «перебору» проти сполук Terminal Services і RDP; SQLRecon для атаки методом «перебору» проти процедури аутентифікації SQL.

В автоматизованих програмах вгадування і злому пароля використовується кілька підходів. Метод «перебору» забирає найбільше часу і є найбільш ефективним. При цьому перебираються всі можливі комбінації символів для пароля при заданому наборі символів (наприклад, abcda | ABCDa | 1234a | !@#$) і максимальній довжині пароля.

Словникові атаки проводяться в припущенні, що більшість паролів складається з цілих слів, дат і чисел, взятих із словника. Для інструментів на

базі словникових атак потрібно вхідний словниковий список. Internet можна завантажити різні безкоштовні і комерційні бази даних зі спеціалізованими словниками (наприклад, англійський словник, спорт і навіть лексика «Зоряних воєн»).

При змішаному методі угадування паролів передбачається, що адміністратори мережі вимагають від користувачів, щоб пароль хоча б трохи відрізнявся від терміна зі словника. Правила гібридного вгадування відрізняються у різних інструментах, але в більшості змішуються символи нижнього і верхнього регістрів, додаються цифри в кінці пароля, слова вводяться в зворотному порядку або з граматичними помилками, використовуються такі символи, як @!#. Гібридний режим реалізований в програмах John the Ripper і Cain & Abel.

2) Скидання пароля. Нерідко зломщикам буває простіше скинути пароль, ніж вгадати його. Багато програми вгадування пароля насправді скидають пароль. У більшості випадків зломщик завантажується з дискети або компакт-диска, щоб обійти звичайні засоби захисту Windows. Більшість програм скидання пароля містять завантажувальну версію Linux, яка монтує томи NTFS і допомагає виявити і скинути пароль адміністратора.

Широко використовуваний інструмент скидання пароля — безкоштовна програма ntpasswd, Петера Нордаль-Хагена. Популярний комерційний продукт — Winternals ERD Commander, один з інструментів пакета Winternals Administrator's Pak . Слід пам'ятати, що більшість інструментів скидають локальні паролі адміністратора тільки в локальних базах даних SAM і непридатні для скидання паролів в Active Directory (AD).

3) Злом паролів. Скидання пароля - ефективний підхід, коли потрібен лише доступ до заблокованого комп'ютера, але спроби скидання пароля залучають небажану увагу. Зазвичай злодії віддають перевагу дізнаватися паролі, не скидаючи їх. Злом пароля полягає в перетворенні захопленого хеш пароля (або іншої секретної форми текстового пароля або пакетів «запит-відповідь») в чисто текстовий оригінал. Щоб розкрити пароль, зломщикові необхідні такі інструменти, як екстрактори для розгадування хешу, розрахункові таблиці для пошуку чисто текстових паролів і аналізатори паролів для отримання даних про аутентифікації.

Розгадування хешу. Деякі інструменти злому паролів забезпечують як вилучення, так і злом хеш пароля, але більшості необхідний LM-хеш, щоб почати процес злому. Деякі інструменти придатні для хешів NT. Найбільш поширений екстрактор хеш пароля Windows — сімейство програм Pwdump. За кілька років було випущено багато версій Pwdump, поточна версія — Pwdump4.

Щоб витягти хеші паролів за допомогою Pwdump, необхідно мати

адміністративний доступ до локального або віддаленого комп'ютера і можливість використовувати NetBIOS для підключення до ресурсу admin$. Існують способи обійти остання умова, але при роботі тільки з одним інструментом воно обов'язково. При успішному запуску Pwdump4 витягуються хеши паролів LM-і NT, і, якщо функція відстеження історії паролів Windows активна — все хеші більш старих паролів. За замовчуванням Pwdump відображає хеші паролів на екран, але можна направити вивід в файл, а потім переслати в програму злому паролів.

Багато знарядь злому паролів приймають хеші у форматі Pwdump. У таких інструментах процес злому зазвичай починається з генерації ряду можливих паролів, які потім хешуються і хеші порівнюються з витягнутим хешем.

Розрахункові таблиці. Сучасні програми злому паролів генерують всі можливі паролі та їх хеші в даній системі і вводять результати в таблицю перетворення, іменовану розрахунковою. Витягуючи хеш з цільової системи, зломщик може просто звернутися до розрахункової таблиці і відшукати лише текстовий пароль. Деякі програми (і Web-вузли) за пару секунд зламують будь хеші LM з використанням розрахункової таблиці. Можна придбати дуже великі таблиці, розміри яких становлять від сотень мегабайтів до сотень гігабайт, або генерувати власну з використанням Rainbow Crack . Метод захисту від розрахункових таблиць — відключити хеші LM і використовувати довгі складні паролі.

4) Аналіз паролів. Деякі програми злому паролів аналізують трафік аутентифікації між клієнтом і сервером і витягують хеші паролів, або достатню інформацію для початку процедури злому. Cain & Abel аналізує трафік аутентифікації і зламує витягнуті хеші. Інші програми аналізу і злому паролів — ScoopLM і KerbCrack, які працюють з трафіком аутентифікації Kerberos. Жодна з цих програм не годиться для зламу трафіку аутентифікації NTLNv2.

5) Захоплення паролів. Багато зломщиків захоплюють паролі, просто встановлюючи для реєстрації натискань на клавіші «троянських коней» або одне з багатьох фізичних пристроїв контролю над клавіатурою. Більшість краде паролі.. Крім того, не становить праці перехоплювати паролі з бездротових клавіатур навіть на відстані кварталу.

2. Порядок виконання роботи

2.1. Відкрийте веб-браузер і перейдіть на http://passwordsgenerator.net

2.2. Виберіть параметри, які відповідають політиці вибору пароля.

2.3. Згенеруйте пароль. Чи легко запам'ятати згенерований пароль?

2.4. Використовуючи онлайн-інструмент для створення паролів, створіть паролі на основі випадкових слів. Зауважте, що оскільки слова з'єднані разом, вони не розглядаються як словарні слова.

2.5. Відкрийте веб-браузер і перейдіть на http://preshing.com/20110811/xkcd-password-generator/

2.6. Згенеруйте новий пароль з випадкових слів, натиснувши **Generate Another!** у верхній частині веб-сторінки.

2.7. Чи легко запам'ятати згенерований пароль?

3. Зміст звіту

3.1. Тема і мета роботи.

3.2. Вихідні дані для виконання роботи.

3.3. Результати виконання роботи

3.4. Висновки

Контрольні запитання

1. Назвіть вимоги до надійних паролів?
2. Чи змінюється складність злому паролю методом грубої сили при збільшенні довжини паролю?
3. Що таке політика вибору пароля?
4. Назвіть основні типи атак на пароль.
5. Що таке розрахункові таблиці і як вони використовуються для злому паролю?

Лабораторна робота № 3

Основні команди операційної системи Windows

Мета роботи: вивчити команди й основні інструменти операційної системи Windows.

Необхідні ресурси

- ПК з доступом до Інтернету

1. Теоретичні відомості

Після виконання лабораторної роботи Ви повинні знати:

• загальні командами Windows;

• основні мережні командами й інструментами, такі як:

ping
tracert/traceroute
netstat
ipconfig
route

Освоївши команди Ви зможете використовувати ці команди в текстових файлах, які ще називаються скриптами (англ. «script»); це найпростіший спосіб програмування.

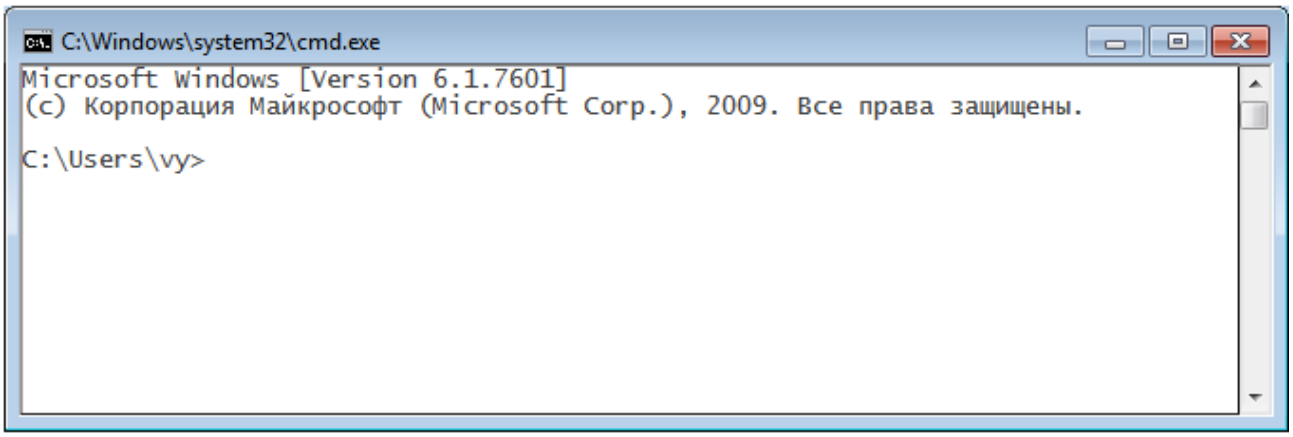
Щоб відкрити вікно командного рядка в ОС Windows:

1. Натисніть кнопку Пуск.

2. Виберіть опцію Виконати (цей пункт відображається як поле для введення символів в меню Пуск в Vista і більш пізніх версіях Windows).

3. Наберіть **cmd** і натисніть **Enter** або **OK**.

4. З'явиться вікно:



5. Тепер Ви можете використовувати команди та інструменти, що наведено нижче.

Команди та інструменти (Windows/DOS)

Команди мають вбудовані функції операційної системи. Інструменти роблять більше: досліджують мережі, шукають хости (англ. «host») (так називаються комп'ютери, підключені до мережі), і дозволяють Вам побачити або встановити інформацію про маршрутизацію вашого хосту.

Команди.

Деякі команди мають коротку і розширену версію.

Команда	Призначення
date	Відображає або встановлює дату
time	Відображає або встановлює час
ver	Відображає версію MS-DOS або Windows
dir	Відображає список вкладених папок і файлів у папці
cls	Очищає екран
mkdir directory або **md directory**	Створює папку з ім'ям directory: md tools
chdir directory або **cd directory**	Заміняє поточну папку на іншу: cd tools
rmdir directory або **rd directory**	Видаляє папку: **rd tools**
tree directory	Відображає структуру файлів і папок у текстово-графічному виді: **tree c:\tools**
chkdsk	Перевіряє диск на наявність помилок і показує звіт
rename source dest або **ren source dest**	Змінює ім'я файлу: ren pictures MyPics
copy source dest	Копіює один або кілька файлів в інше місце: **copy c:\tools\myfile.txt c:\tmp**
move source dest	Переміщає файли й змінює ім'я файлів і папок **move c:\tools c:\tmp**
type file	Відображає зміст одного або більше текстових файлів **type c:\tools\myfile.txt**

more file	Відображає інформацію файлу порціями (скільки вміщується на екран командного рядку за один раз): more **c:\tools\myfile.txt**
delete file або **del file**	Видаляє один або більше файлів: **del c:\tools\myfile.txt**
cd	Для переходу в корінь диска застосовується команда **cd ** Для переходу в будь-який каталог диска застосовується команда **cd [каталог]** (з кореня диска) і команда **cd [\ каталог]** (з будь-якого каталогу або підкаталогу). Для переходу в підкаталог застосовується команда **cd [каталог]** (з каталогу) і команда **cd [каталог / підкаталог]** (з кореня диска). У разі якщо необхідно поміняти не тільки поточний каталог, але і поточний диск, необхідно використовувати ключ **/ D**. Команда буде виглядати так**: cd / D [диск: /]**. Наприклад, перейдемо з папки «Program Files», розташованої на диску «C», на диск «D»: cd / D d: /

Інструменти

Інструмент	Призначення
ping host	Перевіряє з'єднання з хост-машиною. Ця команда посилає ping-пакети протоколу мережевих керуючих повідомлень (англ. «Internet Control Message Protocol», ICMP) іншому комп'ютеру, щоб побачити, скільки часу йому буде потрібно на відповідь та чи відповість він взагалі. Ви можете використати ім'я хосту або його IP адресу. ping google.com ping 172.217.20.206 Можливі варіанти: ping -n 100 google.com відправляє 100 ping-пакетів, та ping -t 216.92.116.13 пінгує хост, поки Ви не натиснете CTRL+C. Щоб побачити більше опцій наберіть: ping /h
tracert host	Відображає маршрут, по якому проходять пакети, щоб добратися до кінцевого хосту. DOS-команда tracert – це адаптація команди traceroute з UNIX. (Команди в DOS могли складатися не більш ніж з восьми символів.) Обидві команди дозволяють Вам знайти маршрут, по якому пакет передається від вашого хосту до іншому. Команда tracert також простежує як довго виконується кожен стрибок і робить, у найкращому разі, 30 стрибків. Часто Ви можете бачити імена машин, через які проходять пакети: **tracert google.com** **tracert 172.217.20.206** Варіанти: **tracert -n 25 google.com** для того, щоб задати максимальну кількість стрибків N, та **tracert -d 172.217.20.206** щоб сховати ім'я хосту. Щоб побачити більше опцій наберіть: **tracert /?**

ipconfig	Відображає інформацію про активні мережеві інтерфейси вашого комп'ютеру (ethernet, ppp, і т.п.). Подібно інструменту ifconfig в Linux. Варіанти: ipconfig /all для одержання більшої інформації. **ipconfig /renew** поновлення мережевого з'єднання, якщо використається автоматична конфігурація протоколу DHCP, і **ipconfig /release** щоб розірвати з'єднання, при використанні DHCP. Більше опцій: **ipconfig /?**
route print	Відображає таблицю маршрутизації. route може також бути використане для налаштування або видалення статичних маршрутів. Варіанти: **route print** відображає список маршрутів, **route delete** видаляє маршрут, та **route add** додає маршрут. Більше варіантів: **route/?**
netstat	Відображає інформацію про статус мережі та встановлює з'єднання з вилученими машинами. Варіанти: **netstat –a** перевіряє всі з'єднання та відображає список портів, що прослуховуються **netstat –n** відображає адреси та номери портів у числовому форматі, і **netstat –e** для простого відображення Ethernet-статистики. Можна використати разом: **netstat -an** Більше варіантів: **netstat/?**

Для одержання додаткової інформації про команди та інструменти у вікні командного рядка введіть:

command /h

command /?

help command

Наприклад, є три способи одержання додаткової інформації про інструмент netstat:

netstat /h

netstat /?

help netstat

2. Порядок виконання роботи.

2.1. Відкрийте вікно CLI.

2.2. Визначите вашу версію DOS або Windows.

2.3. Визначите дату й час системи. Якщо вони невірні, виправте.

2.4. Визначите всі файли та папки на диску c:\.

2.5. Створіть папку c:\cs\lab2. Скопіюйте туди файли з розширенням .sys, або з розширенням ini які є на диску c:\ . Які файли Ви знайшли?

2.6. Визначите IP-адресу вашого комп'ютера.

2.7. Простежте маршрут до сайту **www.google.com**. Визначите IP-адреси проміжних маршрутизаторів.

3. Зміст звіту

3.1. Тема і мета роботи.

3.2. Вихідні дані для виконання роботи.

3.3. Результати виконання роботи (схема, таблиці істинності та часові діаграми.

3.4. Висновки

Контрольні запитання

1. Назвіть призначення програми **ping**
2. Назвіть призначення програми **tracert/traceroute**
3. Назвіть призначення програми **netstat**
4. Назвіть призначення утиліти **ipconfig**
5. Назвіть призначення утиліти **route**

Лабораторна робота № 4

Основні команди операційної системи Linux

Мета роботи: вивчити команди і основні інструменти для операційної системи Linux.

Необхідні ресурси

- ПК з доступом до Інтернету

Після виконання лабораторної роботи Ви повинні знати:

• загальні команди Linux;

• основні мережні командами й інструментами, такі як:

ping

tracert/traceroute

netstat

ifconfig

route

1. Теоретичні відомості

Операційна система: Linux

Як і в Windows, в Linux Ви запускаєте команди у вікні CLI. Ви побачите наступні терміни: консолі (consoles), термінали (terminals) і командні оболонки (shells).

Що Ви можете зробити в командному рядку Linux? Усе, що Ви могли б зробити в будь-якому графічному інтерфейсі, навіть значно більше.

В Linux Ви можете одержати IP однією командою:

ifconfig eth0 192.168.1.205

Як відкрити вікно терміналу.

Так як існує безліч версій Linux, то є кілька способів відкрити вікно консолі.

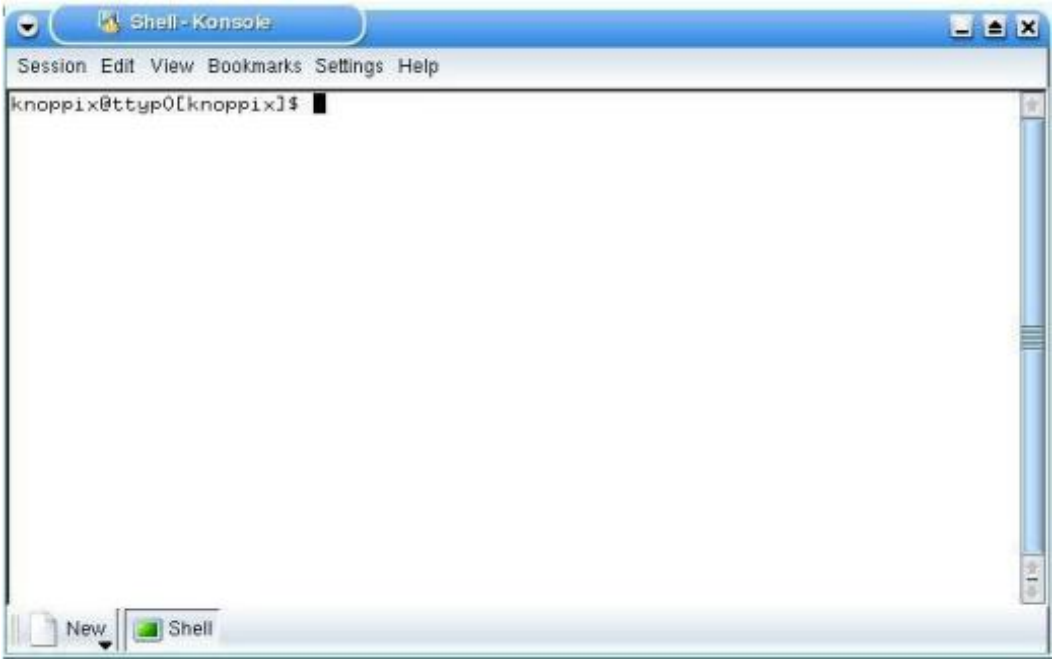
1. Натисніть кнопку Start Application.

2. Якщо Ви бачите “Run Command”, клацніть й уведіть “konsole”, потім Return.

3. Або знайдіть Accessories, потім виберете Terminal.

4. Або ж в багатьох системах Ви можете натиснути CTL-ALT-T.

5. З'явиться вікно схоже на це.



6. Тепер Ви можете використовувати команди та інструменти, що наведено нижче.

Linux команди та інструменти.

Команди

Слова, виділені курсивом, - варіанти, які Ви повинні вводити.

Команда	Призначення
ls	Відображення вмісту поточного каталогу: ls -la Відображення вмісту іншого каталогу: ls -la /etc
cd directory	Перехід з поточного каталогу в каталог з ім'ям directory. Якщо ім'я каталогу не зазначено, то здійснюється перехід у кореневий каталог. Для імені користувача “fred” команда: $cd здійснює перехід у каталог /home/fred, та $cd - перехід в останній відвіданий каталог, та $cd /tmp перехід у каталог /tmp.
cp source dest	Копіювання файлу source у файл dest. Наприклад: cp /etc/passwd /tmp/bunnies копіює файл passwd у файл bunnies

rm file	Видалення файлів. Тільки користувачі з відповідними правами доступу (або користувач root) можуть видалити певні файли. rm letter.txt
mv source dest	Переміщення або перейменування файлів і каталогів. Наприклад: mv secrets.zip innocent.zip
mkdir directory	Створення каталогу з ім'ям directory. Наприклад: mkdir tools
rmdir directory	Видалення каталогу з ім'ям directory, але тільки, якщо він порожній: rmdir tools Додаткове питання: Як Ви видалите каталог з наявними в ньому файлами?
find / -name file	Пошук файлів, починаючи з / (кореня системи), з ім'ям file: find / -name myfile
echo string	Відображення рядка string на екрані: echo hello
command > file	Перенапрямок стандартного виводу на екран команди command у файл file: ls > listing.txt Якщо цей файл уже існує, то він буде затертий, тобто перезаписаний!
command >> file	Перенаправлення стандартного виводу на екран команди **command** у файл **file**. Якщо цей файл уже існує, то інформація записується наприкінці файлу. Наприклад: ls >> listing.txt
man command	Відображення онлайн керівництва про команду command: man ls

Для одержання додаткової інформації про ці команди та інструменти спробуйте наступні варіанти:

command -h
command --help
man command
help command
info command

Наприклад, для одержання додаткової інформації про команду **ls**, введіть кожний з двох можливих варіантів:

ls – help

man ls

Інструменти

Інструменти	Призначення
ping host	Перевірка контакту з хост-машиною: ping www.google.com
traceroute host	Показати шлях, що пройшли пакети, щоб досягти хост-машини: tracert www.google.com
ifconfig	Відображення інформації про активні мережеві інтерфейси (ethernet, ppp, і т.д.).
route	Відображення таблиці маршрутизації.
netstat	Відображення інформації про Ваші мережеві підключення. netstat -an

*Слова, виділені курсивом - це варіанти, які Ви повинні вводити.

2. Порядок виконання роботи

2.1 Визначите власника файлу passwd. (Зверніть увагу: спочатку визначите розташування файлу).

2.2 Створіть каталог work у вашому власному домашньому каталозі (наприклад, якщо Ваш логін - fred, створіть каталог в /home/fred), і скопіюйте файл passwd у каталог work, що Ви тільки що створили. Визначите власника копії passwd.

2.3 Створіть каталог .hide у каталозі work (Зверніть увагу, що ім'я файлу починається із крапки). Подивіться вміст цього каталогу. Що Ви повинні зробити, щоб побачити вміст каталогу .hide?

2.4 Створіть файл test1 зі змістом “Цей файл test1” у каталозі work. Створіть файл test2 зі змістом “Це файл test2” у каталозі work. Скопіюйте у файл із ім'ям test зміст обох попередніх файлів.

3. Зміст звіту

3.1. Тема і мета роботи.

3.2. Вихідні дані для виконання роботи.

3.3. Результати виконання роботи.

3.4. Висновки

Контрольні запитання

1. Назвіть призначення програми **ping**
2. Назвіть призначення програми **tracert/traceroute**
3. Назвіть призначення програми **netstat**
4. Назвіть призначення утиліти **ifconfig**
5. Назвіть призначення утиліти **route**

Лабораторна робота №5

Утиліта netcat

Мета роботи: вивчити можливості утиліти **netcat**

1. Теоретичні відомості

Утиліта nc (або netcat). nc - програма для створення з’єднань з використанням сокетів протоколів TCP і UDP і подальшою передачею даних по ним. Вона дозволяє як здійснювати клієнтські підключення з використанням зазначених протоколів, так і створювати на серверній стороні сокети, що знаходяться в режимі очікування вхідних з’єднань від клієнтів.

Утиліта **netcat** використовується практично для всього, що стосується TCP або UDP. Відкриття TCP з’єднань, посилка UDP пакетів, прослуховування TCP і UDP портів, сканування портів, і робота з версіями IPv4 і IPv6.

Основне застосування:

Сканувати порти;

Перенаправляти порти;

Робити збір банерів сервісів;

Слухати порт (биндить для зворотного з'єднання);

Завантажувати і викачувати файли;

Виводити вміст raw HTTP;

Створити міні-чат;

- і багато іншого.

Існують наступні опції:

-4 Використовувати тільки IPv4 адреси.

-6 Використовувати тільки IPv6 адреси.

-D Включити налагодження на сокеті.

-d Не читати стандартний ввід (stdin).

-h Вивести довідку по nc.

-E Еквівалентно комбінації "-e 'in ipsec esp / transport // require'

-e 'out ipsec esp / transport // require' ", яка включає транспортний режим IPsec ESP в обох напрямках.

-e Якщо підтримка IPsec доступна, то можна вказати використовувану політику IPsec, слідуючи синтаксису, описаного в ipsec_set_policy (3). Якщо необхідно, цей прапор може бути вказаний два рази, по одному правилу для кожного напрямку.

-i interval

Часовий інтервал затримки між надісланими і прийнятими рядками

тексту. Так само задає інтервал затримки між підключеннями до декількох портів.

-k продовжувати слухати (очікувати) наступне з'єднання, після того, як поточне з'єднання було закрито. Помилково використовувати цю опцію без опції -l.

-l слухати вхідні з'єднання, замість підключення до віддаленого хосту. Помилково використовувати цю опцію в зв'язці з опціями -p, -s, або -z. Крім того, будь-який тайм аут вказаний за допомогою опції -w ігнорується.

-n не проводити ніяких перетворень імен та сервісів, в адреси і номери портів.

-o "Once-only режим". За замовчуванням, nc не завершує роботу по сигналу EOF, який надійшов на стандартний ввід, а продовжує роботу до тих пір, поки одна зі сторін не відключиться. ключ –o дозволяє включати підтримку сигналу EOF.

- P proxy_username Ім'я користувача, щоб представитися проксі серверу, який вимагає аутентифікації. Якщо не вказати ім'я користувача, тоді аутентифікація не вдасться. На даний момент проксі аутентифікація можна лише за допомогою HTTP З'ЄДНАННЯ.

-p source_port Вихідний порт, який nc повинен використовувати. Помилково використовувати цю опцію в зв'язці з опцією -l.

-r Вихідні порти і / або порти призначення будуть обрані у випадковому порядку, ніж в послідовному.

-S Включити RFC 2385 TCP MD5 підпис.

-s source_ip_address IP інтерфейсу, який використовується для посилки пакетів.

Помилково використовувати цю опція в зв'язці з опцією -l.

-T ToS Тип обслуговування (ToS) IP для з'єднання. Діючі значення, позначаються ярликами "lowdelay", "throughput", "reliability", або 8-бітними шістнадцятковими значення позначаються, як "0x".

-t Посилати RFC 854 DO NOT і WILL NOT відповіді і DO і WILL запити. Це уможливлює використовувати nc для написання скриптів telnet сесій.

-U Використовувати сокети (Unix Domain Sockets).

-u Використовувати UDP, натомість використовується за замовчуванням TCP.

-v Виводити більше налагоджувальної інформації.

-w timeout Якщо з'єднання і стандартний ввід не використовуються більше ніж заданий тайм аут в секундах, тоді з'єднання закриється. Прапор -w не ефективний с опцією -l, тобто nc буде слухати з'єднання завжди, з або без прапора -w. За замовчуванням тайм аут не заданий.

-X proxy_protocol Використовувати вказаний протокол, для звернення до проксі сервера.

Підтримує протоколи "4" (SOCKS v.4), "5" (SOCKS v.5) і "Connect" (HTTPS proxy). Якщо протокол не вказано, використовується SOCKS 5 версії.

-x proxy_address [: port]

З'єднуватися до хосту використовуючи проксі з адресою. proxy_address і портом port. Якщо port не вказано, тоді будуть використовуватися стандартні порти для проксі протоколу (1080 для SOCKS і 3128 для HTTPS).

-z Сканувати на наявність слухачів демонів, не здійснюючи їм даних.

Помилково використовувати цю опцію в зв'язці з опцією -l.

ім'я хоста може бути вказано у вигляді IP адреси або його імені (якщо не задана опція -n). Зазвичай ім'я хоста повинно бути вказано, крім випадку з використанням опції -l (слухає локальні адреси).

Порти можуть бути вказані по одному, або в діапазоні. Діапазон в форматі nn-mm. Зазвичай порт призначення повинен бути вказаний, крім випадків з використанням опції -U (вказується сокет).

Ім'я хоста може бути вказано у вигляді IP адреси або його імені (якщо не задана опція -n). Зазвичай ім'я хоста повинно бути вказано, крім випадку з використанням опції -l (слухає локальні адреси).

Порти можуть бути вказані по одному, або в діапазоні. Діапазон в форматі nn-mm. Зазвичай порт призначення повинен бути вказаний, крім випадків з використанням опції -U (вказується сокет).

Модель клієнт / сервер

Дуже легко побудувати примітивну модель клієнт / сервер використовуючи nc. На одній консолі запускаємо nc слухати вказаний порт на з'єднання.

Приклад:

$ nc -l 1234

nc слухає порт тисяча двісті тридцять чотири на з'єднання. На другій консолі (або на другий машині) з'єднуємося з машиною на порт, який прослуховується:

$ nc 127.0.0.1 1234

Повинно відбутися з'єднання між портами. Все, що буде набрано на другий консолі, буде відображено на першій і навпаки. Після того, як буде встановлено з'єднання, nc не хвилює, яка зі сторін буде використовуватися, як `server', а яка, як `client'. З'єднання може бути перервано використовуючи EOF (`^ D ').

Передача даних.

Попередній приклад може бути розширений, для побудови передачі даних. Будь-яка інформація спрямована в одну зі сторін з'єднання буде отримана на іншому кінці, і введення і виведення легко можуть бути побудовані в такій послідовності, щоб емулювати передачу даних.

Почніть використовуючи nc для прослуховування порту, з перенаправленням з нього файлу:

$ nc -l 1234> filename.out

Використовуйте другу машину, для підключення до слухача процесу nc, з перенаправленням в нього передається файлу.

$ nc host.example.com 1234 <filename.in

Після передачі файлу, з'єднання автоматично закриється.

Сканування портів

Корисно знати які порти відкриті і які сервіси запущені на досліджуваній машині. Прапор -z може бути використаний, щоб дізнатися про відкриті порту не ініціюючи з'єднання. наприклад:

$ nc -z host.example.com 20-30

Connection to host.example.com 22 port [tcp / ssh] succeeded!

Connection to host.example.com 25 port [tcp / smtp] succeeded!

Був вказаний діапазон портів 20 - 30.

Також це може бути використано, щоб дізнатися який серверний софт запущений, і його версія. Цю інформацію містить вітальне повідомлення.

Як правило, щоб зробити це, спочатку необхідно ініціювати з'єднання, потім обірвати його, коли буде отримано вітання. Це може бути виконано зазначенням маленького тайм ауту за допомогою прапора -w, або можна використовувати команду "QUIT" на сервері:

$ Echo "QUIT" | nc host.example.com 20-30

SSH-1.99-OpenSSH_3.6.1p2

Protocol mismatch.

220 host.example.com IMS SMTP Receiver Version 0.84 Ready

Безпека

Очевидно, що при подібному використанні **netcat** інформація передається по мережі в вихідному нешифрованому вигляді. Для передачі некритичних даних це цілком прийнятно, але при передачі будь-якої цінної інформації розумно використовувати netcat в поєднанні з SSH-тунелем.

Використання SSH-тунелю має дві переваги:

Інформація передається всередині зашифрованого тунелю, так що вона добре захищена;

На сервері не потрібно відкривати ніяких додаткових портів в конфігурації брандмауера, оскільки з'єднання буде встановлено через SSH.

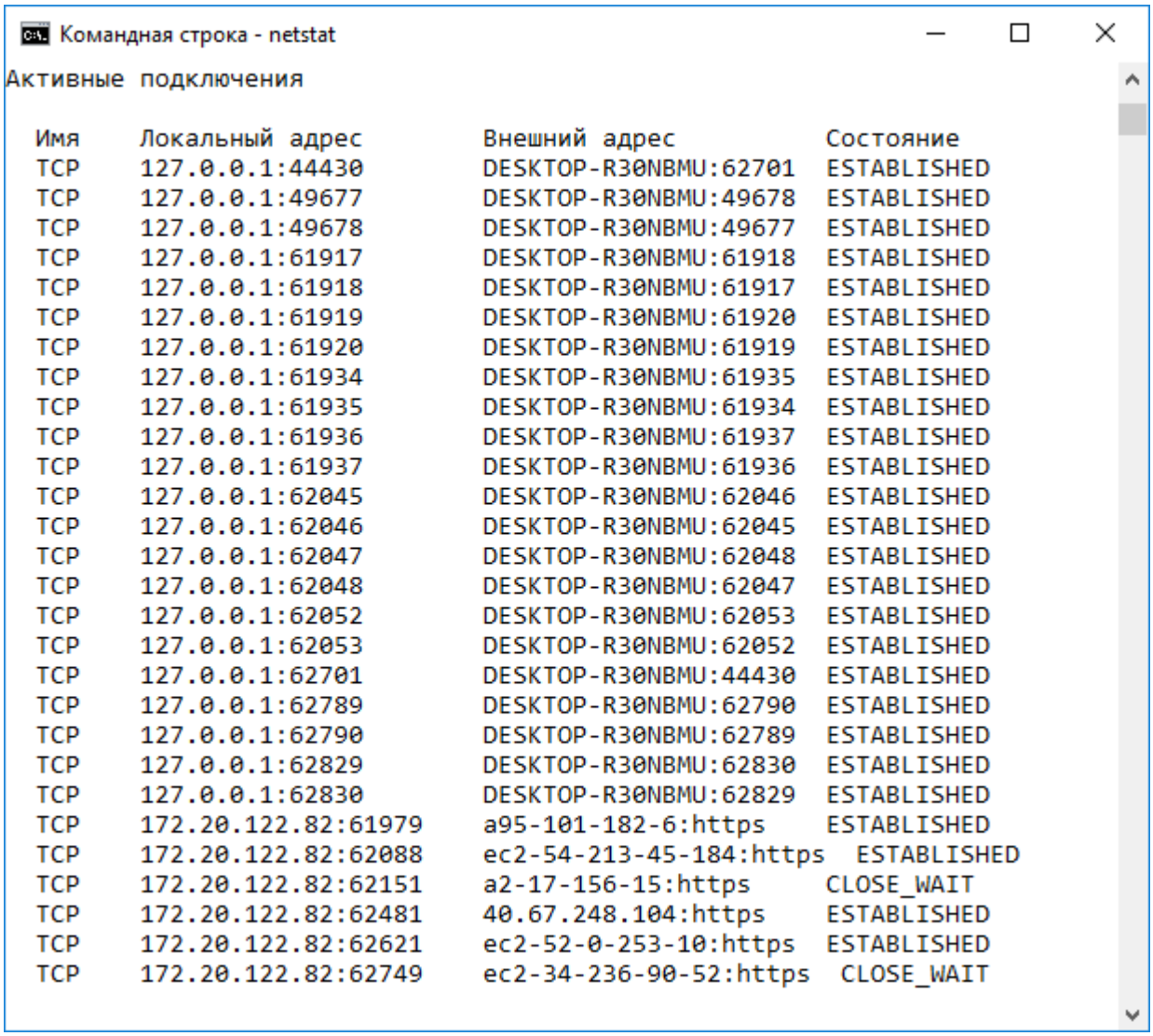
Використовуючи команди вивчені в лабораторній роботі 1 дізнайтеся IP-адресу вашого комп'ютера, мережеву маску, DNS-ім'я хоста і MAC-адресу. Порівняйте інформацію отриману Вами, з інформацією, отриманою Вашим напарником за сусіднім комп’ютером. У чому схожість і в чому різниця? Які IP-адреси використовуються в мережі: публічні або приватні?

1. Команда netstat

Команда **netstat** відображає мережеву статистику: з ким Ви з’єднані, як довго працює мережа і т.п. Щоб запустити утиліту в Linux або Windows потрібно зайти в консоль операційної системи і набрати:

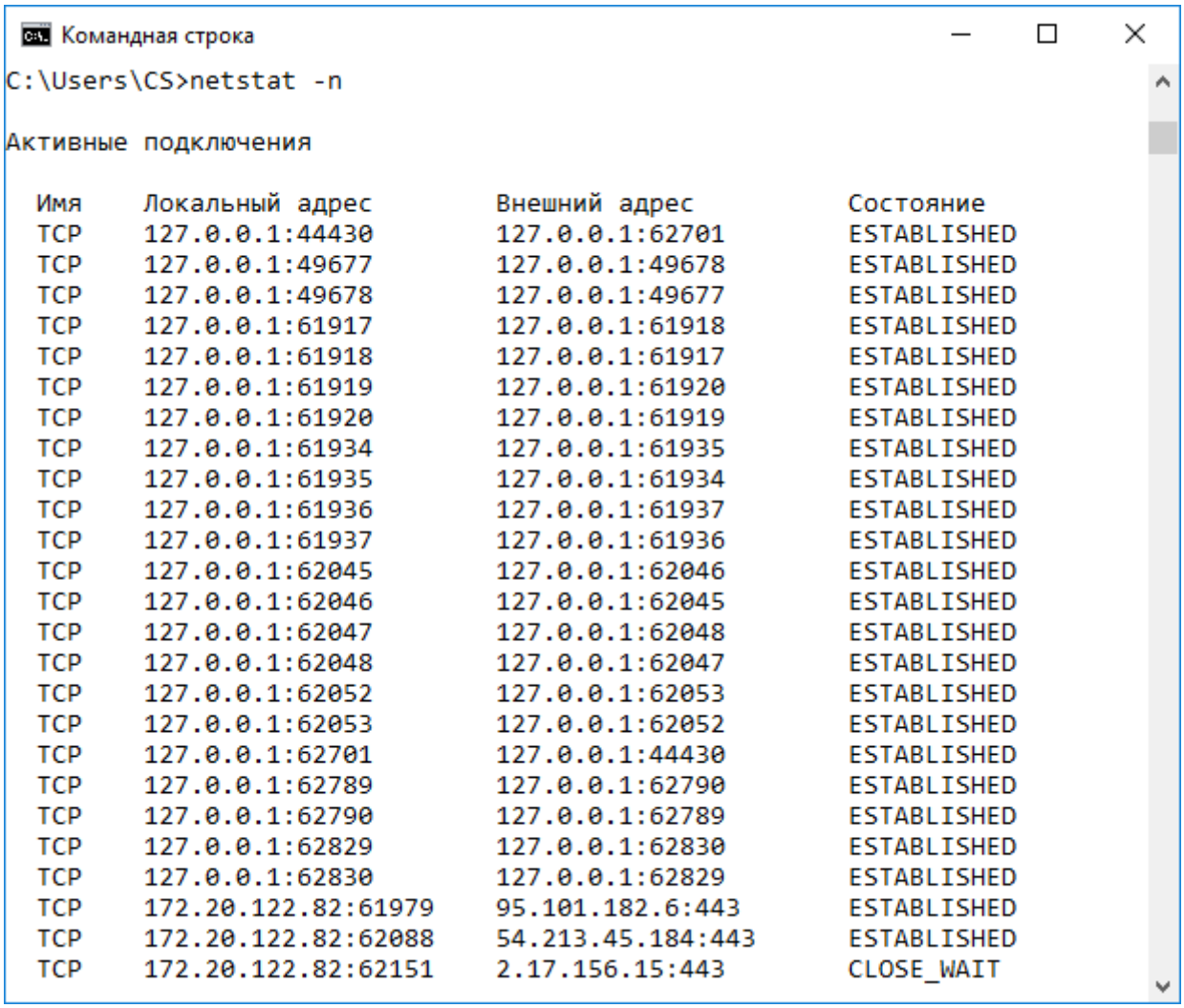
netstat

У консолі Ви побачите список встановлених з'єднань.



Якщо ви хочете, щоб з’єднання відображали адреси і номери портів в числовому форматі, наберіть:

netstat –n



Щоб викликати довідку команди, наберіть:

netstat –h

Для того, щоб побачити список усіх з’єднання та портів, що знаходяться в стані очікування, наберіть:

netstat –an

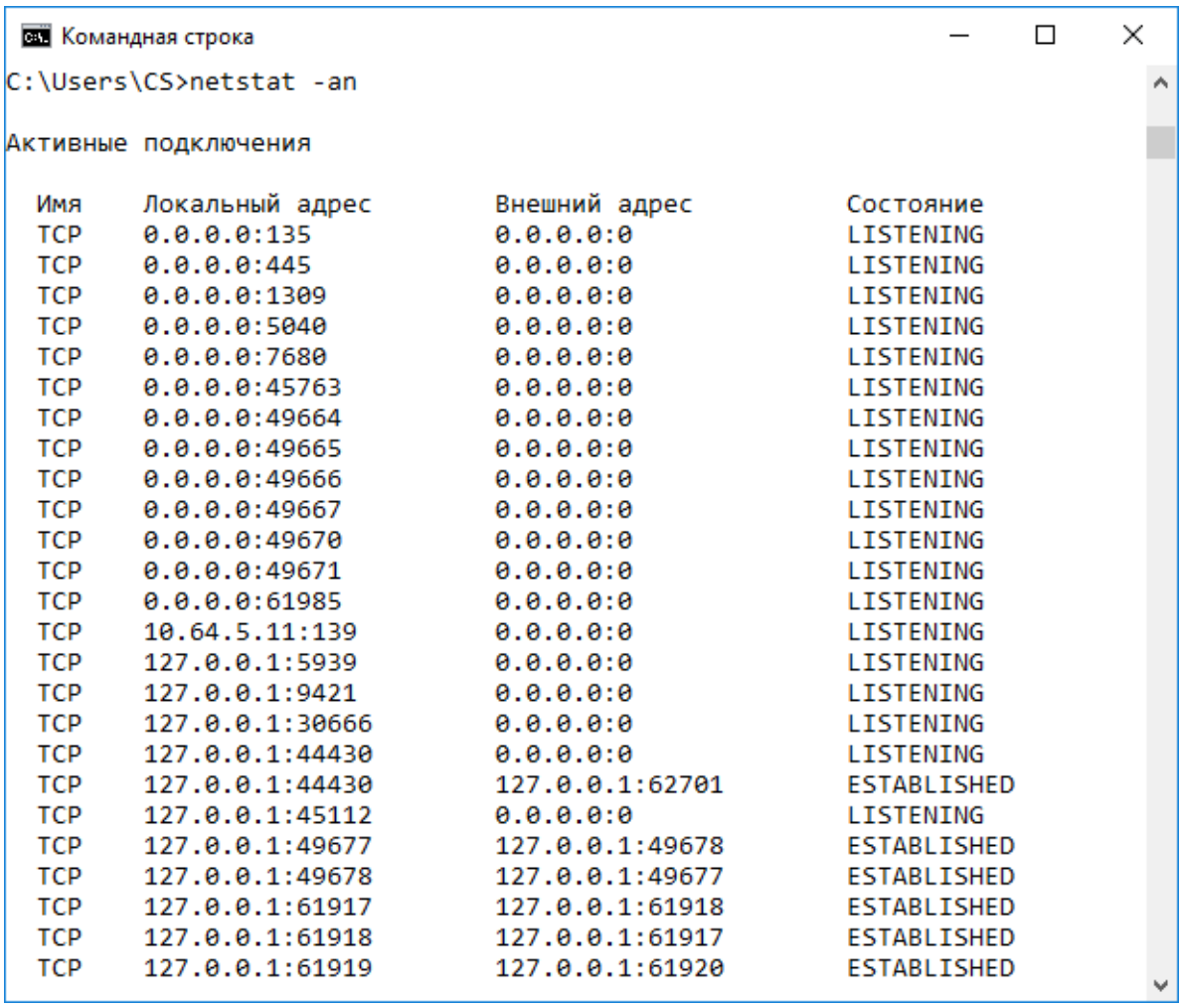
Стан (State) LISTEN (LISTENING) показує пасивно відкриті з’єднання . Саме вони і надають мережеві служби.

ESTABLISHED – це встановлені з’єднання, тобто мережеві служби в процесі їх використання.

У списку **netstat**, зверніть увагу на колонки, в яких наведено і локальний і віддалений IP- адреси і подивіться які порти використовують дані підключення:

Proto Recv-Q Send-Q Local Address Foreign Address (state)

tcp4 0 0 192.168.2.136:1043 66.220.149.94:443 ESTABLISHED



Порти це цифри, які наведені після IP-адреси, відокремлені двокрапкою. Чому порти використовуються віддаленими адресами відрізняються від портів, які використовують локальні адреси?

Відкрийте кілька вікон в браузері і в кожному з них відкрийте різні сайти. Знову використовуйте утиліту netstat.

Коли відкрито кілька вкладок в одному браузері, як він може зрозуміти якій з них передавати отриману інформацію?

Чому відбувається так, що коли використовується браузер, то зникають порти, що знаходяться в процесі прослуховування?

Які протоколи використовуються?

Що станеться, якщо один протокол буде використовуватися більше одного разу одночасно?

2. Порядок виконання роботи

Для того, щоб виконати ці вправи, Вам знадобиться програма netcat (nc). У дистрибутиві (BackTrack) Kali Linux вона є за умовчанням, проте її легко можна завантажити і встановити і на інші операційні системи.

2.1. У консолі наберіть:

nc -h

Ця команда відобразить опції, які доступні в netcat.
Для створення простого серверу в Linux / Windows, наберіть:

nc -l -p 1234

Ви тільки що запустили сервер, що прослуховує порт 1234.

2.2. Відкрийте друге вікно в консолі та наберіть:

netstat –a

Так Ви перевірите, що з'явився новий сервіс, що прослуховує порт 1234.
Щоб встановити зв'язок з сервером потрібно використовувати клієнт! У другому вікні консолі наберіть:

nc localhost 1234

Дана команда створить з'єднання з сервером на порт 1234. Тепер, все, що друкується в одному з відкритих вікон консолі буде відображатися і в іншому.

Як можна використати подібну службу, аби зламати вашу систему? Netcat пересилає весь трафік у відкритому вигляді. Чи існує безпечна альтернатива?

3. Зупиніть сервер, повернувшись в перше вікно консолі і натиснувши Ctrl + C.

4. Тепер, створіть текстовий файл (. txt) і назвіть його «test». Запишіть у текстовий файл фразу: “Welcome to my server!”

Як тільки закінчите, подивіться на команду і розберіться в ній і розкажіть Вашому викладачеві, що робить кожна з її опцій.
Наберіть:

nc -l -p 1234 < test

З іншого вікна консолі підключіться до серверу, набравши:

nc localhost 1234

Коли клієнт підключиться до серверу, Ви повинні побачити вміст файлу test.

Який протокол використовується для підключення до серверу? Чи дозволяє netcat Вам це змінити? Якщо так, то яким чином?

3. Зміст звіту

3.1. Тема і мета роботи.

3.2. Вихідні дані для виконання роботи.

3.3. Результати виконання роботи.

3.4. Висновки

Контрольні запитання

1. Назвіть основні застосування утиліту netstat
2. Що таке порт?
3. Чому порти використовуються віддаленими адресами відрізняються від портів, які використовують локальні адреси?
4. Коли відкрито кілька вкладок в одному браузері, як він може зрозуміти якій з них передавати отриману інформацію?
5. Чому відбувається так, що коли використовується браузер, то зникають порти, що знаходяться в процесі прослуховування?

Лабораторна робота № 6

Службові програми - утіліти

Мета роботи: вивчити службові програми - утиліти (ipconfig, ping, traceroute, netstat, telnet та ін.).

Необхідні ресурси

- ПК з доступом до Інтернету

1. Теоретичні відомості

В операційних системах Microsoft Windows **ipconfig** - це утиліта командного рядка для виводу деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS. Також є подібні графічні утиліти: **winipcfg** і **wntipcfg** (остання передувала ipconfig).

Утиліта **ipconfig** дозволяє визначати, які значення конфігурації були отримані за допомогою DHCP, APIPA або іншої служби IP-конфігурації або задані адміністратором вручну.

Часто в операційних системах Linux і UNIX деталі з'єднання відслідковуються декількома утилітами, головною серед них є **ifconfig**. Проте, **ipconfig** поряд з **ifconfig** присутній в Mac OS X, там **ipconfig** команда сервісу як оболонка до агента IP Configuration і може використовуватися для контролю BootP і DHCP клієнта з CLI.

Здебільшого, команда Ipconfig використовується з командного рядка, але її також можна відкрити, перейшовши за адресою C:\WINDOWS\system32, і запустити exe-файл "ipconfig.exe".

Можливі параметри

Параметр	**Значення**
/all	Відтворення повної інформації про всі адаптери та параметри з'єднань.
/release	Обнулення параметрів з'єднання, скинення IP, маски, шлюзу, DNS.
/release *[адаптер]*	Відправка повідомлення DHCPRELEASE DHCP-серверу для вивільнення поточної конфігурації DHCP та видалення конфігурації IP-адреса для видалення адаптеру (або ж усіх адаптерів, якщо він не заданий). Цей параметр відключає протокол TCP/IP для адаптерів, котрі отримують автоматично IP-адресу.

/renew	Скинення та отримання IP-адреси для певного адаптера, а якщо адаптер не вказаний - то для всіх. Доступне тільки за умови автоматичного отримання IP-адреси.
/flushdns	Очищення DNS кешу.
/registerdns	Оновлення всіх зарезервованих адрес DHCP та переєрестрація імен DNS.
/displaydns	Відображення вмісту кешу DNS.
/showclassid *[адаптер]*	Відображення коду класу DHCP для вказанного адаптеру. Доступне тільки за умови автоматичного отримання IP-адреси.
/setclassid *[адаптер] [код_класу]*	Зміна коду класу DHCP. Доступне тільки за умови автоматичного отримання IP-адреси.
/?	Довідка.

2. Порядок виконання роботи

Завдання 1. Перегляд мережевих налаштувань

1. За допомогою утиліти ipconfig (запускається в командному рядку командою ipconfig) визначите IP-адресу й маску підмережі для свого комп'ютера.
2. Визначте клас підмережі, у якій перебуває ваш комп'ютер без використання маски підмережі й по масці підмережі.
3. Визначте адресу підмережі, у якій перебуває ваш комп'ютер, з використанням функції "Логічне І" над IP- адресою й маскою підмережі. Слід мати на увазі, що операція "Логічне І" повинна проводитися із двійковим значенням операндів.

Завдання 2.

За допомогою утиліти ping (запускається в командному рядку командою ping) перевірте доступність хостів, мінімальний, середній і максимальний час приймання-передачі ICMP пакетів до них. Можна розглянути хости, наприклад у наступній послідовності:

1. Сервер вашого безпосереднього провайдера або сервера вашої підмережі;
2. Який-небудь сервер вашого регіону;

3. Веб-сервер Університету в Кембриджі: www.cam.ac.uk;

4. Веб-сервер Інтернет-Університету Інформаційних Технологій: www.intuit.ru;

5. Веб-сервер Університету в Каліфорнії: www.ucla.edu;

6. Веб-сервер Університету в Токіо: www.u-tokio.ac.jp;

7. Веб-сервер компанії Майкрософт: www.microsoft.com.

Зверніть увагу, що в останньому випадку Icmp-пакети блокуються веб-сервером.

Завдання 3.

За допомогою утиліти tracert (запускається в командному рядку командою tracert) визначите маршрути проходження й час проходження пакетів до хостів, наведених у завданні 2.

Завдання 4

1. За допомогою утиліти netstat (запускається в командному рядку командою netstat) подивитеся активні поточні мережні підключення і їх стан на вашому комп'ютері.

2. Запустіть кілька екземплярів веб-браузера, завантаживши в них веб-сторінки з різних веб-серверів. Подивитеся за допомогою netstat, які нові мережні підключення з'явилися в списку.

3. Закривайте браузери й за допомогою netstat перевіряйте зміну списку мережних підключень.

Завдання 5. Ознайомлення із протоколом HTTP за допомогою утиліти telnet

1. Запустіть сеанс telnet (запускається в командному рядку командою telnet). При цьому з'явиться підказка Microsoft Telnet>. З повним списком команд можна ознайомитися за допомогою команди help.

2. Дозвольте режим відображення символів, що вводяться із клавіатури, за допомогою команди set localecho.

3. Відповідно до протоколу HTTP необхідно встановити з'єднання з веб-сервером. Для цього за допомогою команди open установлюється з'єднання, наприклад: open www.yandex.ru 80.

4. Сформуйте клієнтський запит. Як мінімум він повинен містити рядок стану, наприклад:

GET HTTP://WWW.YANDEX.RU/INDEX.HTML HTTP/1.0

Якщо поля запиту відсутні, то введення закінчується двома натисканнями клавіші **<ENTER>** для вставки порожнього рядка після заголовка.

Слід звернути увагу на те, що при введенні не можна допускати помилок, оскільки при спробі їх виправити за допомогою клавіші **<BACKSPACE>**, її натискання інтерпретується як частина запиту.

5. Вивчіть отриману відповідь сервера. Зверніть увагу на код відповіді в рядку стану відповіді веб-сервера в рядку стану й поля заголовка відповіді. Якщо відповідь сервера дуже велика (у першу чергу через розмір документа в тілі відповіді), то вміст відповіді сервера у вікні інтерпретатора командного рядка обрізується з початку. У цьому випадку рекомендується для перегляду заголовка замість методу GET використовувати метод HEAD.

3. Зміст звіту

3.1. Тема і мета роботи.

3.2. Вихідні дані для виконання роботи.

3.3. Результати виконання роботи.

3.4. Висновки

Контрольні завдання

1. За допомогою якої утиліти по заданому доменному імені хоста можна визначити його IP адреса? Визначте IP адреса хоста www.kyivstar.ua

2. З допомогою утиліти telnet визначите який веб-сервер встановлений на хості www.ukr.net.

Визначте маршрут проходження ICMP пакетів до хоста www.ttt.com. Визначите географічну локалізацію хоста.

Лабораторна робота № 7

Визначення затримки мережі за допомогою утиліт «ping» і «traceroute»

Мета роботи: виміряти і оцінити затримку мережі за певний час і скласти наочні приклади типової активності мережі

2. Порядок виконання роботи

Для цього проаналізуєте затримку віддаленого комп'ютера за допомогою команди ping. Використовуючи час затримки в мілісекундах, обчисліть середню затримку і діапазон (мінімальне і максимальне значення) тривалості затримки.

Завдання 1: Реєстрація затримки мережі за допомогою утиліти «ping».

У частині 1 вам потрібно обчислити затримку мережі при зверненні до кількох веб-сайтів, розташованим в різних країнах. Цю процедуру можна використовувати в корпоративній мережі університету для формування базового рівня продуктивності.

Крок 1: Перевірка підключення.

Для перевірки підключення відправте наступні ехо-запити за допомогою команди ping на веб-сайти регіонального Інтернет-реєстру (RIR):

C: \ Users \ User1> ping www.arin.net

C: \ Users \ User1> ping www.lacnic.net

C: \ Users \ User1> ping www.afrinic.net

C: \ Users \ User1> ping www.apnic.net

Примітка. Оскільки веб-сайт www.ripe.net не відповідає на запити ICMP, в цій лабораторній роботі він не використовується.

Крок 2: Зберіть мережеві дані.

Вам необхідно зібрати достатню кількість даних для підрахунку статистики застосування команди **ping**, відправивши по 25 ехо-запитів на

кожну адресу, вказану в кроці 1.

Збережіть результати за всіма веб-сайтів в текстові файли.

2.1. У вікні командного рядка введіть **ping** для отримання списку доступних параметрів.

C:\Users\User1> ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]

[-r count] [-s count] [[-j host-list] | [-k host-list]]

[-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:

-t Ping the specified host until stopped.

To see statistics and continue - type Control-Break;

To stop - type Control-C.

-a Resolve addresses to hostnames.

-n count Number of echo requests to send.

-l size Send buffer size.

-f Set Don't Fragment flag in packet (IPv4-only).

-i TTL Time To Live.

-v TOS Type Of Service (IPv4-only. This setting has been deprecated

<output omitted>

2.2. Використовуючи команду ping з функцією підрахунку, відправте 25 exo-запитів на вузол призначення, як показано нижче. При цьому в цій папці буде створено файл з ім’ям arin.txt. Цей текстовий файл буде містити результати exo-запитів за допомогою команди ping.

C: \ Users \ User1> ping -n 25 www.arin.net> arin.txt

Примітка. Поле терміналу залишається порожнім до повного виконання команди, так як її результати перенаправляються в текстовий файл arin.txt (в даному прикладі). Символ > використовується для перенаправлення виведених на екрані даних в текстовий файл і перезапису цього файлу, якщо він вже існує. Якщо в файл необхідно зберегти кілька результатів, в рядку команди замініть > на >>.

2.3. Виконайте команду ping для інших веб-сайтів.

C:\Users\User1> ping –n 25 www.afrinic.net > afrinic.txt

C:\Users\User1> ping –n 25 www.apnic.net > apnic.txt

C:\Users\User1> ping –n 25 www.lacnic.net > lacnic.txt

Крок 3: Перевірте зібрані дані.

Для перегляду результатів, збережених в створеному файлі, у вікні командного рядка введіть more.

```
C:\Users\User1> more arin.txt
Pinging www.arin.net [192.149.252.76] with 32 bytes of data:
Reply from 192.149.252.76: bytes=32 time=108ms TTL=45
Reply from 192.149.252.76: bytes=32 time=114ms TTL=45
Reply from 192.149.252.76: bytes=32 time=112ms TTL=45
<output omitted>
Reply from 192.149.252.75: bytes=32 time=111ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
Ping statistics for 192.149.252.75:
Packets: Sent = 25, Received = 25, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 107ms, Maximum = 121ms, Average = 111ms
```

Примітка. Натисніть ПРОБІЛ, щоб відобразити іншу частину файлу, або клавішу q, щоб вийти.

Щоб перевірити, чи створені необхідні файли, введіть команду dir, яка виводить на екран список всіх файлів в папці. Щоб відобразити тільки текстові файли, можна використовувати спеціальний символ *.

```
C:\Users\User1> dir *.txt
Volume in drive C is OS
Volume Serial Number is 0A97-D265
Directory of C:\Users\User1
02/07/2013  12:59 PM         1,642 afrinic.txt
02/07/2013  01:00 PM         1,615 apnic.txt
02/07/2013  12:40 PM         1,641 arin.txt
02/07/2013  12:58 PM         1,589 lacnic.txt
4 File(s)        6,487 bytes
0 Dir(s)  34,391,453,696 bytes free
```

Внесіть отримані результати в наведену нижче таблицю.

	Мінімальне	Максимальне	Середнє
www.afrinic.net			
www.apnic.net			
www.arin.net			
www.lacnic.net			

Порівняйте результати затримки. Наскільки час затримки залежить від географічного розташування?

Завдання 2: Реєстрація затримки мережі за допомогою утиліти «traceroute».

Залежно від зони охоплення вашого Інтернет-провайдера і розташування вузлів джерела і призначення відслідковувані маршрути можуть перетинати безліч переходів і мереж. Для визначення затримки мережі можна також використовувати команду traceroute. У частині 2 команда tracert застосовується для відстеження шляху до тих же вузлів призначення, що і в частині 1.

Для цієї мети команда tracert використовує пакети з повідомленням ICMP TTL Exceed (Час життя пакету перевищено) і ехо-відгуки ICMP.

1: Скористайтеся командою «tracert» і збережіть отримані результати в текстові файли.

Скопіюйте наступні команди, щоб створити файли відстеження маршруту для кожного вузла:

C:\Users\User1> tracert www.arin.net > traceroute_arin.txt

C:\Users\User1> tracert www.lacnic.net > traceroute_lacnic.txt

C:\Users\User1> tracert www.afrinic.net > traceroute_afrinic.txt

C:\Users\User1> tracert www.apnic.net > traceroute_apnic.txt

2: Введіть команду «more», щоб перевірити відстежені маршрути.

2.1 Введіть команду more, щоб переглянути вміст цих файлів:

C:\Users\User1> more traceroute_arin.txt

Tracing route to www.arin.net [192.149.252.75]

over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 192.168.1.1

2 11 ms 12 ms 11 ms 10.39.0.1

3 10 ms 15 ms 11 ms 172.21.0.116

4 19 ms 10 ms 11 ms 70.169.73.90

5 13 ms 10 ms 11 ms chnddsrj01-ae2.0.rd.ph.cox.net [70.169.76.229]

6 72 ms 71 ms 70 ms mrfddsrj02-ae0.0.rd.dc.cox.net [68.1.1.7]

7 72 ms 71 ms 72 ms 68.100.0.146

8 74 ms 83 ms 73 ms 172.22.66.29

9 75 ms 71 ms 73 ms 172.22.66.29

10 74 ms 75 ms 73 ms wsip-98-172-152-14.dc.dc.cox.net [98.172.152.14]

11 71 ms 71 ms 71 ms host-252-131.arin.net [192.149.252.131]

12 73 ms 71 ms 71 ms www.arin.net [192.149.252.75]

Trace complete.

У цьому прикладі отримання відповіді від основного шлюзу зайняло менше 1 мс (192.168.1.1). В рядку лічильника переходів 6 зазначено, що шлях до вузла 68.1.1.7 і назад зайняв в середньому 71 мс. Шлях до кінцевому вузлу www.arin.net і назад зайняв в середньому 72 мс.

Між рядками 5 і 6 спостерігається велика затримка в мережі, про що свідчить збільшення середнього часу проходження сигналу туди і назад з 11 до 71 мс.

2.2. Аналогічним чином проаналізуйте інші результати застосування команди tracert.

Який висновок можна зробити про залежність часу проходження сигналу в обох напрямках і географічного місцезнаходження вузла?

Завдання 1. Перегляд мережевих налаштувань

1. За допомогою утиліти ipconfig (запускається в командному рядку командою ipconfig) визначите IP-адресу й маску підмережі для свого комп'ютера.
2. Визначте клас підмережі, у якій перебуває ваш комп'ютер без використання маски підмережі й по масці підмережі.
3. Визначте адресу підмережі, у якій перебуває ваш комп'ютер, з використанням функції "Логічне І" над IP-адресою й маскою підмережі. Слід мати на увазі, що операція "Логічне І" повинна проводитися із двійковим значенням операндів.

Завдання 2

За допомогою утиліти ping перевірте доступність хостів, мінімальний, середній і максимальний час приймання-передачі ICMP пакетів до них.

Можна розглянути хости, наприклад у наступній послідовності:

1. Сервер вашого безпосереднього провайдера або сервера вашої підмережі;
2. Який-небудь сервер вашого регіону;
3. Веб-сервер Університету в Кембриджі: www.cam.ac.uk;
4. Веб-сервер Інтернет-Університету Інформаційних Технологій: www.intuit.ru;
5. Веб-сервер Університету в Каліфорнії: www.ucla.edu;
6. Веб-сервер Університету в Токіо: www.u-tokio.ac.jp;
7. Веб-сервер компанії Майкрософт: www.microsoft.com.

Зверніть увагу, що в останньому випадку Icmp-пакети блокуються веб-сервером.

Внесіть отримані результати в таблицю:

	Мінімальне	Максимальне	Середнє
Сервер вашої підмережі			
www.cam.ac.uk			
www.intuit.ru			
www.ucla.edu			
www.u-tokio.ac.jp;			
www.microsoft.com.			

Завдання 3.

За допомогою утиліти **tracert** (запускається в командному рядку командою **tracert**) визначите маршрути проходження й час проходження пакетів до хостів, наведених у завданні 2.

3. Зміст звіту

3.1. Тема і мета роботи.

3.2. Вихідні дані для виконання роботи.

3.3. Результати виконання роботи.

3.4. Висновки

Контрольні запитання.

1. Результати використання команд **tracert** і **ping** можуть дати важливу інформацію про затримку мережі. Що необхідно для того, щоб отримати точну картину основних даних по затримках мережі?

2. Як можна використовувати отримані основні показники?

3. За допомогою якої утиліти по заданому доменному імені хоста можна визначити його IP адреса? Визначте IP адреса хоста www.kyivstar.ua

4. З допомогою утиліти **telnet** визначите який веб-сервер встановлений на хості www.ukr.net

5. Визначте маршрут проходження ICMP пакетів до хоста www.ttt.com. Визначите географічну локалізацію хоста.

Підписано до друку 28.09.2018 р.
Формат 60х90/16. Гарнітура Times.
Папір офсетний. Друк на дублікаторі.
Умов. – друк. арк. 1,95. Обл. – вид. арк.2.0.
Зам. № М064-18
Тираж 50 прим.

Видавець та виготовлювач
Тернопільський національний економічний університет
вул. Львівська, 11, м. Тернопіль, 46009
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців ДК № 3467 від 23.04.2009 р.
Видавничо-поліграфічний центр «Економічна думка ТНЕУ»
вул. Бережанська, 2, м. Тернопіль, 46009
тел. (0352) 47-58-72
E-mail: edition@tneu.edu.ua.