Міністерство освіти і науки України
Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до виконання лабораторних робіт з навчальної дисципліни

«КОМП'ЮТЕРНІ МЕРЕЖІ»

для студентів денної та заочної форми навчання
галузі Інформаційні технології.

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки та
програмного забезпечення, протокол
№ 1 від 26.08.2025 року

Кропивницький
2025

Комп’ютерні мережі: методичні рекомендації до виконання лабораторних робіт для студентів денної форми навчання галузі 12 «Інформаційні технології» / М-во освіти і науки України, Центральноукр. нац. техн. ун-т; [уклад. О.В. Коваленко, А.С. Коваленко, К.Д. Авраменко, М.Ю. Черкашин] – Кропивницький: ЦНТУ, 2025. – 86 с.

Укладачі:

Коваленко О.В., докт. техн. наук, доц;

Коваленко А.С. канд. техн. наук, доц;

Авраменко К.Д. Lead Back-End Developer\Architect, Швейцарія м. Цюріх;

Черкашин М.Ю. керівник операцій підтримки абонентських сервісів, архітектор хмарної та датацентричної інфраструктури ІСП Імперіал м. Кропивницький.

Рецензенти: Смірнов О. А., докт. техн. наук, професор, завідувач кафедри;
Якименко Н.М., к. ф.-м. наук, доцент.

ЗМІСТ

ВСТУП

Навчальний курс «Комп'ютерні мережі» призначений для набуття теоретичних знань та практичних навичок роботи з локальними та глобальними комп'ютерними мережами. Розглядаються питання архітектури мережі, топології мережі, протоколи, функціонування та будови локальних та глобальних комп'ютерних мереж.

Метою викладання навчальної дисципліни «**Комп'ютерні мережі**» є забезпечення здобувачів вищої освіти комплексом знань, умінь та навичок, необхідних для застосування в професійній діяльності у сфері роботи з локальними та глобальними комп'ютерними мережами.

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Лабораторні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд 501, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету. Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, студенту необхідно мати комп'ютерну техніку (з виходом у Internet) та оргтехніку для комунікації з викладачами, виконання тестових завдань в системі дистанційної освіти.

Лабораторне заняття – форма навчального заняття, спрямована на закріплення та вдосконалення студентом теоретичних знань, отриманих як на лекційних і практичних заняттях, так і в процесі самостійного вивчення матеріалу.

Провідна форма навчання – лекція. Лекція дозволяє дуже економно, з мінімальними затратами часу і викладача, і студентів, надати великий обсяг інформації по темі, що розглядається. За характером логіки пізнання впроваджуються аналітичний, індуктивний та дедуктивний методи.

Супровідні методи – лабораторні роботи.

Основна дидактична мета практичного заняття – закріплення й деталізація знань, а головне – формування навичок і вмінь. Для проведення практичного заняття викладач готує відповідні методичні матеріали: тести для виявлення рівня оволодіння необхідними теоретичними положеннями ; набір практичних завдань різної складності для розв'язування їх на занятті та дидактичні засоби.

Під час лабораторного заняття студенти під керівництвом викладача набувають практичних навичок у роботі з обчислювальною технікою, оволодівають методикою створення програмних продуктів у програмному середовищі. При цьому у студентів формуються вміння й практичні навички використання різних програмних засобів ПК для розв’язання конкретних економічних задач відповідно до індивідуального завдання.

Проведення лабораторних занять ґрунтується на попередньо підготовлених методичних матеріалах: визначення підготовленості студентів до виконання завдань лабораторного заняття на основі тестового контролю знань основних положень теорії досліджуваної теми, усного контролю виконання домашнього завдання, пов'язаного з розробкою макетів документів, які необхідно розробити програмно під час заняття.

Індивідуальні завдання до кожної лабораторної роботи мають чітко виражену прикладну спрямованість, що враховує профіль підготовки студентів, тобто охоплюють питання автоматизації рішення різних завдань економіки і підприємництва.

На лабораторному занятті студенти під керівництвом викладача проводять розробку ПЗ в навчальних лабораторіях з використанням комп'ютерної техніки. Основною метою лабораторного заняття є практичне підтвердження окремих теоретичних положень та набуття практичних вмінь з виконання обчислювальних експериментів.

Головна особливість цих занять полягає у тому, що вони об'єднують теорію з практикою, забезпечують їх єдність. Сукупність лабораторних занять з дисципліни є лабораторним практикумом, що сплановане за єдиним

задумом. Лабораторні заняття плануються після проведення лекцій. А при необхідності розробки програм, проектування баз даних або підготовки складних розрахунків і початкових даних перед лабораторними заняттями проводяться консультації.

Лабораторні роботи виконуються у такій послідовності:

– вивчення навчального матеріалу з теми лабораторної роботи з використанням конспекту лекцій, рекомендованих підручників і навчальних посібників;

– самостійна підготовка студентами макетів інтерфейсів програм, які мають бути практично створені на занятті;

– виконання завдання на ПК відповідно до виданого варіанта й подання результатів викладачеві.

По завершенню кожної роботи студенти готують і оформлюють звіт й захищають отримані результати.

Звіт повинен містити:

– тему й мету роботи;

– зміст завдання й короткий опис порядку його виконання;

– аналіз отриманих результатів та висновки роздруківку основних результатів виконання індивідуального завдання.

Напередодні проведення кожного лабораторного заняття (після відповідної лекції) студентам видається завдання, що містить: тему і мету заняття; скорочені теоретичні відомості щодо змісту лабораторного заняття; список питань для підготовки (це можуть бути контрольні питання по темі, що вивчається, заповнення роздатних матеріалів індивідуальними даними, розробка програм, таблиць і т.д.); послідовність підлягаючих виконанню на занятті дій (завдання на лабораторну роботу); вимоги до змісту звіту. Студент повинен вивчити навчальний матеріал, завдання, підготувати необхідні для роботи на занятті матеріали і знать відповіді на контрольні питання.

У ході підготовки може бути створена заготовка звіту, що дозволить заощадити час на занятті. Лабораторні заняття проводяться в аудиторіях, академічна група ділиться на підгрупи.

Усі лабораторні заняття з дисципліни проводяться фронтально, кожний студент працює за окремим комп'ютером. На початку заняття, після оголошення теми, цільової установки і коротких указівок щодо особливостей роботи викладачем проводиться контроль підготовленості студентів, звичайно, шляхом перевірки відповідей на контрольні питання (тестів), рідше, у формі усної бесіди по темі заняття.

Для контролю може використовуватися і тестування. Обов'язково перевіряється наявність матеріалів для виконання роботи (програм, роздаткового матеріалу з відпрацьованими індивідуальними питаннями, початкових даних для вирішення задач, заготовок звіту і т. п.).

За відсутності матеріалів, необхідних для виконання роботи, і знань, які не дозволяють виконати роботу, студент до роботи не допускається, і йому пропонується виконати необхідну підготовку. Сама робота повинна виконуватися у додатковий час. У ході заняття студенти самостійно виконують передбачені завданням дії, заносячи результати в звіт. На це відводиться до 85–90% часу заняття.

Викладач здійснює контроль за роботою і надає допомогу при виникненні ускладнень, звертає увагу на складні ключові моменти. Причому основну увагу приділяється не вказівці на конкретну помилку, а методиці пошуку причин виникнення цих помилок.

Складання звіту – це відповідальний етап лабораторного заняття. При його складанні студенти розвивають навики аналізу, узагальнення і творчого осмислення результатів роботи, а також навики розробки документації до програмного продукту. Необхідно прагнути до того, щоб студенти оформляли звіт про виконану роботу і представили його викладачу до кінця лабораторної роботи.

Цьому сприяє наявність наперед підготовленої заготовки, в яку послідовно заносяться всі необхідні дані і зроблені висновки.

Звіт повинен бути представлений у вигляді електронного документа. За наслідками контролю готовності студентів до роботи, об'єму і правильності її виконання, повноти і якості оформлення звіту і його захисту, терміну захисту викладач виставляє оцінку.

Звіти, які не представлені під час заняття, захищаються в додатковий час. В окремих випадках оцінка може виставлятися за групу взаємопов'язаних робіт.

При оцінці лабораторної роботи викладач ураховує правильність та розуміння роботи розроблених програмних продуктів, уміння працювати у програмному середовищі. Оцінки за кожну лабораторну роботу вносяться у відповідний журнал.

Студент, що пропустив лабораторне заняття або не допущений до нього, зобов'язаний виконати відповідну роботу під час самостійної підготовки і відзвітувати. Повторна здача робіт, які не були прийняті, проводиться під час консультацій або під час наступних лабораторних занять.

Оцінки, отримані студентом за окремі лабораторні заняття враховуються при виставленні поточної модульної оцінки з навчальної дисципліни.

У процесі лабораторного заняття викладач організує такі види методичної роботи зі студентами:вирішення поточних запропонованих індивідуальних завдань на лабораторну роботу; перевірку завдань щодо розробки програм та алгоритмів; захист лабораторних робіт окремих студентів.

Перелік тем лабораторних занять наведено у табл. 1.

Таблиця 1 – Перелік тем лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма навчання	заочна форма навчання (повна, бакалавр)
1	ЛР 1. Використання консольних діагностичних засобів в мережах TCP/IP.	6	0,5
2	ЛР 2. Основи налаштування маршрутизаторів різних фірм виробників	6	0,5
3	ЛР 3. Робота та аналіз мережної клієнт-серверної взаємодії	6	0,5
4	ЛР 4. Дослідження мережевих топологій з використанням Cisco Packet Tracer	6	0,5
5	ЛР 5. Вивчення сервісів локальної мережі	6	0,5
6	ЛР 6. Дослідження характеристик та параметрів бездротової мережі WI-FI	6	0,5
7	ЛР 7. Сканування IP-мереж з довільною кількістю об'єктів та визначення їх властивостей	6	0,5
8	ЛР 8. Базове перехоплення і аналіз мережевого трафіку в локальній мережі	6	0,5
Усього годин		**48**	**4**

Лабораторна робота №1

ТЕМА: ВИКОРИСТАННЯ КОНСОЛЬНИХ ДІАГНОСТИЧНИХ ЗАСОБІВ В МЕРЕЖАХ TCP/IP

МЕТА: Отримати практичні навики роботи з мережними системними утилітами ARP, NETSTAT, IPCONFIG, Ping, Tracert (Traceroute у ОС Linux), Nslookup, Telnet, SHH.

ЗНАТИ: Основи використання та консольної роботи з обраної ОС

ТЕОРЕТИЧНІ ВІДОМОСТІ

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором):

– Мережна утиліта Ipconfig (Windows): https://uk.wikipedia.org/wiki/Ipconfig.

– Мережна утиліта Ifconfig (Linux): https://uk.wikipedia.org/wiki/Ifconfig.

– Мережна утиліта Netstat: https://uk.wikipedia.org/wiki/Netstat.

– Мережна утиліта ARP: https://uk.wikipedia.org/wiki/ARP.

– Консоль Windows: https://uk.wikipedia.org/wiki/Інтерфейс_командного_рядка.

– Консоль Linux: https://uk.wikipedia.org/wiki/Bash.

– https://uk.wikipedia.org/wiki/TCP/IP.

– https://uk.wikipedia.org/wiki/Ping.

– https://uk.wikipedia.org/wiki/Traceroute.

– https://uk.wikipedia.org/wiki/Nslookup.

– https://uk.wikipedia.org/wiki/Доменна_система_імен.

– https://uk.wikipedia.org/wiki/Telnet.

– https://uk.wikipedia.org/wiki/SHH.

ЗАВДАННЯ

ЧАСТИНА 1. Використовуючи мережні утиліти (IPCONFIG, NETSTAT, ARP) визначити дані локального ПК та заповнити наступні таблиці (1.1-1.4):

Таблиця 1.1 Ipconfig

НАЗВА	ЗНАЧЕННЯ
Ім'я комп'ютера	
Опис	
Фізична адреса	
Локальний IPv6-адресу каналу	
IPv4-адрес	
Маска під мережі	
Основний шлюз	
DHCP-сервер	
DNS-сервери	

Таблиця 1.2. Netstat

НАЗВА	ЗНАЧЕННЯ
Статистика IPv4	
Отримано пакетів	
Отримано помилок у заголовках	
Отримано помилок в адресах	
Направлено датаграмм	
Отримано невідомих протоколів	
Відкинуто отриманих пакетів	
Доставлено отриманих пакетів	
Запитів на виведення	
Відкинуто маршрутів	
Відкинуто вихідних пакетів	
Вихідних пакетів без маршруту	
Статистика TCP для IPv4	
Активних відкрито	
Пасивних відкрито	
Збоїв при підключенні	
Скинуто підключень	
Поточних підключень	
Отримано сегментів	
Відправлено сегментів	
Повторно відправлено сегментів	
Статистика UDP для IPv4	

Отримано датаграмм	
Відсутність портів	
Помилки при отриманні	
Відправлено датаграмм	

Таблиця 1.3. Netstat

IPv4 таблиця маршрутів. Активні маршрути:				
Мережний адрес	Маска мережі	Адреса шлюзу	Інтерфейс	Метрика

Таблиця1.4. arp

Адреса в Інтернеті	Фізична адреса	Тип

ЧАСТИНА 2. Використовуючи мережу утиліту Ping (перевірка з'єднання в мережах на основі TCP/IP) отримати задані дані проаналізувати їх та додати результати до звіту.

2.1 ПАРАМЕТРИ ЗАПИТУ МЕРЕЖНОЇ УТИЛІТИ PING:

– Запит до серверу (www.cityofsydney.nsw.gov.au).

(Відправити 1 ехо запит. Розмір буфера відправки 1000.)

– Запит до серверу (paris.com).

(Відправити 20 ехо запитів. Розмір буфера відправки 1000.)

– Запит до серверу (www.newyork.com).

(Відправити 20 ехо запитів. Розмір буфера відправки 1000.)

Використовуючи мережу утиліту Tracert (визначення маршрутів прямування даних в мережах TCP/IP) отримати задані дані проаналізувати їх та додати результати до звіту.

2.2 ПАРАМЕТРИ ЗАПИТУ МЕРЕЖНОЇ УТИЛІТИ TRACERT:

– Запит до серверу (www.cityofsydney.nsw.gov.au).

(Максимальне число стрибків при пошуку вузла. 100.)

– Запит до серверу (www.paris.com).

(Максимальне число стрибків при пошуку вузла. 100.)

– Запит до серверу (www.newyork.com).

(Максимальне число стрибків при пошуку вузла. 100.)

Використовуючи мережу утиліту nslookup (звернення до системи DNS) отримати задані дані проаналізувати їх та додати результати до звіту.

2.3 ПАРАМЕТРИ ЗАПИТУ МЕРЕЖНОЇ УТИЛІТИ TRACERT:

– Отримати дані сайту www.ukr.net, за допомогою DNS серверу google-public-dns-a.google.com [8.8.8.8].

ЧАСТИНА 3.

3.1 За допомогою системної утиліти Telnet (інсталювати за необхідності) підключитись до виданого сервера та визначити можливості та необхідність сервера.

Сервер обирати з таблиці 3.1 (https://telnet.org/htm/places.htm) відповідно до індивідуального варіанту завдання студента.

Визначити свій індивідуальний варіант завдання - відповідно до списку наданого у курсі “Комп’ютерні мережі”, розділ «Лабораторні роботи» (дистанційне навчання ЦНТУ https://moodle.kntu.kr.ua/course/view.php?id=1035)

3.2. За допомогою системної утиліти ssh. Виконати дії Level0-Level5 за посиланням https://overthewire.org/wargames/bandit/bandit0.html.

Таблиця 3.1 Список серверів Telnet

№	ПОСИЛАННЯ
1.	horizons.jpl.nasa.gov 6775 :: NASA JPL HORIZONS solar system data
2.	rainmaker.wunderground.com 3000 :: weather via telnet!
3.	nyancat.dakko.us :: ANSI art animation of "poptart cat"
4.	mapscii.me :: a Telnet interface to a Braille/ASCII map renderer
5.	india.colorado.edu 13 (Get the time) :: get the time
6.	telnet.wmflabs.org :: telnet gateway to wikimedia content
7.	telehack.com 23 :: Telehack
8.	telehack.com :: Telehack - web
9.	freechess.org 5000 :: freechess.org
10.	towel.blinkenlights.nl 23 :: Star Wars asciimation
11.	towel.blinkenlights.nl 666 :: The Bofh Excuse Server

№	ПОСИЛАННЯ
12.	mtrek.com:1701 :: mtrek (star trek themed game)
13.	xmltrek.com:1701 :: xmltrek (star trek themed game)
14.	bbs.archaicbinary.net :: Archaic Binary
15.	ateraan.com 4002 :: New Worlds - Ateraan
16.	avalon-rpg.com 23 :: Avalon: The Legend Lives
17.	aardmud.org 4000 :: Aardwolf MUD
18.	bbs.armageddonbbs.com 23 :: Armageddon BBS
19.	52.88.68.92 1234 :: Cuban Bar
20.	TextMMOde.com 23 :: Sands of Time / Deep Space MMO
21.	legendofthereddragon.ca 23 :: Legend of the Red Dragon (Canada)
22.	lord.stabs.org 23 :: Legend of the Red Dragon
23.	thehatshop.mudhosting.net 3000 :: Hallowed Halls
24.	eclipse.cs.pdx.edu 7680 :: New Moon
25.	batmud.bat.org 23 :: BatMUD
26.	forgottenkingdoms.org 4000 :: Forgotten Kingdoms
27.	mush.shelteringcolorado.com 2601 :: Sheltering Sky: Colorado by Night
28.	igormud.org 1701 :: Igor MUD/
29.	zombiemud.org 23 :: Zombie MUD
30.	achaea.com 23 :: Achaea, Dreams of Divine Lands
31.	gcomm.com 23 :: Galacticomm BBS
32.	1984.ws 23 :: 1984

ОФОРМЛЕННЯ ЗВІТУ

У звіт лабораторної роботи помістити:

– Завдання л/роботи.

– Покрокові матеріали що повністю підтверджують виконання л/роботи (текст, таблиці, принтскріни, та інші матеріали для підтвердження виконання л/роботи).

– Короткі змістовні відповіді на л/роботи.

Лабораторну роботу оформляти по загальноприйнятій формі (ДСТУ) та аналогічно до інших предметів кафедри КБПЗ ЦНТУ.

КОНТРОЛЬНІ ЗАПИТАННЯ

ARP (Address Resolution Protocol)

1. Що таке протокол ARP, і для чого він використовується в комп'ютерних мережах?
2. Як команда arp -a допомагає в діагностиці мережі? Яку інформацію вона надає?
3. Які проблеми можуть виникнути при неправильно налаштованих записах ARP?

NETSTAT (Network Statistics)

4. Що таке netstat і які основні завдання виконує ця утиліта?
5. Поясніть значення ключів -a, -n, -o у команді netstat.
6. Як за допомогою netstat можна визначити, які порти на вашому комп'ютері є відкритими?

IPCONFIG (IP Configuration)

7. Яка мета команди ipconfig і яку інформацію вона надає?
8. Як за допомогою команди ipconfig /all можна отримати детальну інформацію про конфігурацію мережі?
9. Яким чином команда ipconfig /release та ipconfig /renew можуть бути корисними при вирішенні проблем з підключенням?

Ping (Packet Internet Groper)

10. Що таке утиліта ping і для чого вона використовується?
11. Що означає показник часу відповіді (RTT) у результатах ping?
12. Як використання команди ping допомагає визначити доступність віддаленого хоста?

Tracert (Trace Route)

13. Яка мета команди tracert і як вона працює?
14. Що таке "TTL" (Time to Live) і яку роль він відіграє в роботі tracert?
15. Як за допомогою tracert можна діагностувати проблеми з маршрутизацією?

Nslookup (Name Server Lookup)

16. Яка основна функція утиліти nslookup?
17. Як за допомогою nslookup можна визначити IP-адресу певного доменного імені?
18. Що таке "reversed nslookup" і як він працює?

Telnet

19. Що таке протокол Telnet і для чого він використовується?
20. Які ризики безпеки пов'язані з використанням Telnet?
21. Як команда telnet може бути використана для перевірки доступності певного порту на віддаленому сервері?

SSH (Secure Shell)

22. Чим SSH відрізняється від Telnet і які переваги він має?
23. Як відбувається автентифікація при використанні SSH?
24. Що таке SSH-ключі і як вони покращують безпеку підключень?

Лабораторна робота №2

ТЕМА: ОСНОВИ НАЛАШТУВАННЯ МАРШРУТИЗАТОРІВ РІЗНИХ ФІРМ ВИРОБНИКІВ

МЕТА: Отримати практичні навики роботи з інтерфейсами маршрутизаторів різних фірм виробників

ЗНАТИ: Основи використання веб браузеру обраної ОС

ТЕОРЕТИЧНІ ВІДОМОСТІ

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором):

– Виробник Mikrotik https://mikrotik.com/.

– Виробник TP-LINK https://www.tp-link.com.

– Виробник Tenda https://www.tendacn.com.

– Виробник Asus https://www.asus.com.

– Виробник linksys https://www.linksys.com/.

– Виробник mercusys https://www.mercusys.com.

Таблиця 2.1 Список емуляторів мережного обладнання

№	БРЕНД	НАЗВА ПРИСТРОЮ	ГІПЕРПОСИЛАННЯ
1.	Mikrotik	Всі моделі в одному емуляторі	https://demo.mt.lv/
2.	Apple	Wi-fi Router	http://chasms.com/osx/yosemite/apu1.htm
3.	netis	Всі моделі в одному емуляторі	https://www.netisru.com/Uploads/Support/Emulators/overseas/welcome.htm
4.	Asus	RT-N10E (Old Interface)	https://www.wisp.pl/al/demo/RT-N10E/home.htm
5.	Asus	RT-N12 (Old Interface)	https://event.asus.com/2009/networks/dummy_ui/rt-n12/
6.	Asus	RT-N16 (Old Interface)	https://event.asus.com/2009/networks/dummy_ui/rt-n16/
7.	Asus	RT-N56U (Old Interface)	https://event.asus.com/2009/networks/dummy_ui/en/
8.	Asus	RT-AC5300 (New Interface)	https://demoui.asus.com/
9.	Netgear	WNDR3400v3	https://highspeed.tips/files/emulators/netgear_genie/start.html
10.	TP-LINK	(MiFi) M7350	https://www.tp-link.com/uk-ua/support/emulator/
11.	TP-LINK	(MiFi) M7200	https://www.tp-link.com/uk-ua/support/emulator/
12.	TP-LINK	(MiFi) M7000	https://www.tp-link.com/uk-ua/support/emulator/
13.	TP-LINK	(MiFi) M5250	https://www.tp-link.com/uk-ua/support/emulator/

№	БРЕНД	НАЗВА ПРИСТРОЮ	ГІПЕРПОСИЛАННЯ
14.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE650	https://www.tp-link.com/uk-ua/support/emulator/
15.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE605X	https://www.tp-link.com/uk-ua/support/emulator/
16.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE600X	https://www.tp-link.com/uk-ua/support/emulator/
17.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE455	https://www.tp-link.com/uk-ua/support/emulator/
18.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE450	https://www.tp-link.com/uk-ua/support/emulator/
19.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE500X	https://www.tp-link.com/uk-ua/support/emulator/
20.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE505X	https://www.tp-link.com/uk-ua/support/emulator/
	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE330	https://www.tp-link.com/uk-ua/support/emulator/
21.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE365	https://www.tp-link.com/uk-ua/support/emulator/
22.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE305	https://www.tp-link.com/uk-ua/support/emulator/
23.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE300	https://www.tp-link.com/uk-ua/support/emulator/
24.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE230	https://www.tp-link.com/uk-ua/support/emulator/
25.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE190	https://www.tp-link.com/uk-ua/support/emulator/
26.	TP-LINK	(Підсилювачі Wi-Fi сигналу) RE200	https://www.tp-link.com/uk-ua/support/emulator/
27.	TP-LINK	(Підсилювачі Wi-Fi сигналу) TL-WA830RE	https://www.tp-link.com/uk-ua/support/emulator/
28.	TP-LINK	(Підсилювачі Wi-Fi сигналу) TL-WA860RE	https://www.tp-link.com/uk-ua/support/emulator/
29.	TP-LINK	(Підсилювачі Wi-Fi сигналу) TL-WA855RE	https://www.tp-link.com/uk-ua/support/emulator/
30.	TP-LINK	(Підсилювачі Wi-Fi сигналу) TL-WA854RE	https://www.tp-link.com/uk-ua/support/emulator/
31.	TP-LINK	(Підсилювачі Wi-Fi сигналу) TL-WA850RE	https://www.tp-link.com/uk-ua/support/emulator/
32.	TP-LINK	(Підсилювачі Wi-Fi сигналу) TL-WA730RE	https://www.tp-link.com/uk-ua/support/emulator/
33.	TP-LINK	(Адаптери Powerline) TL-WPA8631P KIT	https://www.tp-link.com/uk-ua/support/emulator/
34.	TP-LINK	(Адаптери Powerline) TL-WPA7617 KIT	https://www.tp-link.com/uk-ua/support/emulator/
35.	TP-LINK	(Адаптери Powerline)TL-WPA7517 KIT	https://www.tp-link.com/uk-ua/support/emulator/
36.	TP-LINK	(Адаптери Powerline)TL-WPA4220 KIT	https://www.tp-link.com/uk-ua/support/emulator/
37.	TP-LINK	(3G/4G маршрутизатори) Archer MR500	https://www.tp-link.com/uk-ua/support/emulator/
38.	TP-LINK	(3G/4G маршрутизатори) Archer MR600	https://www.tp-link.com/uk-ua/support/emulator/
39.	TP-LINK	(3G/4G маршрутизатори) Archer MR400	https://www.tp-link.com/uk-ua/support/emulator/
40.	TP-LINK	(3G/4G маршрутизатори) Archer MR200	https://www.tp-link.com/uk-ua/support/emulator/
41.	TP-LINK	(3G/4G маршрутизатори) TL-MR3420	https://www.tp-link.com/uk-ua/support/emulator/
42.	TP-LINK	(3G/4G маршрутизатори) TL-MR150	https://www.tp-link.com/uk-ua/support/emulator/
43.	TP-LINK	(3G/4G маршрутизатори) TL-MR100	https://www.tp-link.com/uk-ua/support/emulator/
44.	TP-LINK	(3G/4G маршрутизатори) TL-MR6400	https://www.tp-link.com/uk-ua/support/emulator/
45.	TP-LINK	(3G/4G маршрутизатори) TL-MR3020	https://www.tp-link.com/uk-ua/support/emulator/

№	БРЕНД	НАЗВА ПРИСТРОЮ	ГІПЕРПОСИЛАННЯ
46.	TP-LINK	(3G/4G маршрутизатори) TL-MR3040	https://www.tp-link.com/uk-ua/support/emulator/
47.	TP-LINK	(3G/4G маршрутизатори) TL-WR942N	https://www.tp-link.com/uk-ua/support/emulator/
48.	TP-LINK	(3G/4G маршрутизатори) TL-WR842N	https://www.tp-link.com/uk-ua/support/emulator/
49.	TP-LINK	(3G/4G маршрутизатори) TL-MR3220	https://www.tp-link.com/uk-ua/support/emulator/
50.	TP-LINK	(Точки доступу) TL-WA901ND	https://www.tp-link.com/uk-ua/support/emulator/
51.	TP-LINK	(Точки доступу) TL-WA801N	https://www.tp-link.com/uk-ua/support/emulator/
52.	TP-LINK	(Точки доступу) TL-WA801ND	https://www.tp-link.com/uk-ua/support/emulator/
53.	TP-LINK	(Точки доступу) TL-WA701ND	https://www.tp-link.com/uk-ua/support/emulator/
54.	TP-LINK	(Точки доступу) TL-WA5110G	https://www.tp-link.com/uk-ua/support/emulator/
55.	TP-LINK	(Комутатори L3/L2) SG3428MP	https://www.tp-link.com/uk-ua/support/emulator/
56.	TP-LINK	(Комутатори L3/L2) TL-SG3428MP	https://www.tp-link.com/uk-ua/support/emulator/
57.	TP-LINK	(Комутатори L3/L2) TL-SX3008F	https://www.tp-link.com/uk-ua/support/emulator/
58.	TP-LINK	(VPN-маршрутизатори) TL-ER6120	https://www.tp-link.com/uk-ua/support/emulator/
59.	TP-LINK	(VPN-маршрутизатори) TL-ER6020	https://www.tp-link.com/uk-ua/support/emulator/
60.	TP-LINK	(VPN-маршрутизатори) TL-ER604W	https://www.tp-link.com/uk-ua/support/emulator/
61.	TP-LINK	(VPN-маршрутизатори) TL-R600VPN	https://www.tp-link.com/uk-ua/support/emulator/
62.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX11000	https://www.tp-link.com/uk-ua/support/emulator/
63.	TP-LINK	(Wi-Fi маршрутизатори) Archer GX90	https://www.tp-link.com/uk-ua/support/emulator/
64.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX90	https://www.tp-link.com/uk-ua/support/emulator/
65.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX6000	https://www.tp-link.com/uk-ua/support/emulator/
66.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX72	https://www.tp-link.com/uk-ua/support/emulator/
67.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX73	https://www.tp-link.com/uk-ua/support/emulator/
68.	TP-LINK	(Wi-Fi маршрутизатори) Archer Air R5	https://www.tp-link.com/uk-ua/support/emulator/
69.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX55 Pro	https://www.tp-link.com/uk-ua/support/emulator/
70.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX53	https://www.tp-link.com/uk-ua/support/emulator/
71.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX55	https://www.tp-link.com/uk-ua/support/emulator/
72.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX50	https://www.tp-link.com/uk-ua/support/emulator/
73.	TP-LINK	(Wi-Fi маршрутизатори) Archer A8	https://www.tp-link.com/uk-ua/support/emulator/
74.	TP-LINK	(Wi-Fi маршрутизатори) Archer C80	https://www.tp-link.com/uk-ua/support/emulator/
75.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX23	https://www.tp-link.com/uk-ua/support/emulator/
76.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX20	https://www.tp-link.com/uk-ua/support/emulator/
77.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX1500	https://www.tp-link.com/uk-ua/support/emulator/
78.	TP-LINK	(Wi-Fi маршрутизатори) Archer AX10	https://www.tp-link.com/uk-ua/support/emulator/

№	БРЕНД	НАЗВА ПРИСТРОЮ	ГІПЕРПОСИЛАННЯ
79.	TP-LINK	(Wi-Fi маршрутизатори) Archer A64	https://www.tp-link.com/uk-ua/support/emulator/
80.	TP-LINK	(Wi-Fi маршрутизатори) Archer C64	https://www.tp-link.com/uk-ua/support/emulator/
81.	TP-LINK	(Wi-Fi маршрутизатори) Archer C50	https://www.tp-link.com/uk-ua/support/emulator/
82.	TP-LINK	(Wi-Fi маршрутизатори) Archer C54	https://www.tp-link.com/uk-ua/support/emulator/
83.	TP-LINK	(Wi-Fi маршрутизатори) Archer C6U	https://www.tp-link.com/uk-ua/support/emulator/
84.	TP-LINK	(Wi-Fi маршрутизатори) Archer C1200	https://www.tp-link.com/uk-ua/support/emulator/
85.	TP-LINK	(Wi-Fi маршрутизатори) Archer C24	https://www.tp-link.com/uk-ua/support/emulator/
86.	TP-LINK	(Wi-Fi маршрутизатори) Archer A2	https://www.tp-link.com/uk-ua/support/emulator/
87.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR802N	https://www.tp-link.com/uk-ua/support/emulator/
88.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR844N	https://www.tp-link.com/uk-ua/support/emulator/
89.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR820N	https://www.tp-link.com/uk-ua/support/emulator/
90.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR841N	https://www.tp-link.com/uk-ua/support/emulator/
91.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR845N	https://www.tp-link.com/uk-ua/support/emulator/
92.	TP-LINK	(Wi-Fi маршрутизатори) Archer C3200	https://www.tp-link.com/uk-ua/support/emulator/
93.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR1043ND	https://www.tp-link.com/uk-ua/support/emulator/
94.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR1043N	https://www.tp-link.com/uk-ua/support/emulator/
95.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR740N	https://www.tp-link.com/uk-ua/support/emulator/
96.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR741ND	https://www.tp-link.com/uk-ua/support/emulator/
97.	TP-LINK	(Wi-Fi маршрутизатори) Archer C3150	https://www.tp-link.com/uk-ua/support/emulator/
98.	TP-LINK	(Wi-Fi маршрутизатори) Archer C7	https://www.tp-link.com/uk-ua/support/emulator/
99.	TP-LINK	(Wi-Fi маршрутизатори) Archer A9	https://www.tp-link.com/uk-ua/support/emulator/
100.	TP-LINK	(Wi-Fi маршрутизатори) Archer C4000	https://www.tp-link.com/uk-ua/support/emulator/
101.	TP-LINK	(Wi-Fi маршрутизатори) Archer A7	https://www.tp-link.com/uk-ua/support/emulator/
102.	TP-LINK	(Wi-Fi маршрутизатори) Archer C3150 V2	https://www.tp-link.com/uk-ua/support/emulator/
103.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR842ND	https://www.tp-link.com/uk-ua/support/emulator/
104.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR841ND	https://www.tp-link.com/uk-ua/support/emulator/
105.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR842N	https://www.tp-link.com/uk-ua/support/emulator/
106.	TP-LINK	(Wi-Fi маршрутизатори) Archer C2300 Touch P5	https://www.tp-link.com/uk-ua/support/emulator/
107.	TP-LINK	(Wi-Fi маршрутизатори) Archer C59	https://www.tp-link.com/uk-ua/support/emulator/
108.	TP-LINK	(Wi-Fi маршрутизатори) Archer C58	https://www.tp-link.com/uk-ua/support/emulator/
109.	TP-LINK	(Wi-Fi маршрутизатори) Archer C5400X	https://www.tp-link.com/uk-ua/support/emulator/
110.	TP-LINK	(Wi-Fi маршрутизатори) Archer C25	https://www.tp-link.com/uk-ua/support/emulator/
111.	TP-LINK	(Wi-Fi маршрутизатори) Archer C20i	https://www.tp-link.com/uk-ua/support/emulator/

№	БРЕНД	НАЗВА ПРИСТРОЮ	ГІПЕРПОСИЛАННЯ
112.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR1045ND	https://www.tp-link.com/uk-ua/support/emulator/
113.	TP-LINK	(Wi-Fi маршрутизатори) TL-WDR4300	https://www.tp-link.com/uk-ua/support/emulator/
114.	TP-LINK	(Wi-Fi маршрутизатори) TL-WDR3600	https://www.tp-link.com/uk-ua/support/emulator/
115.	TP-LINK	(Wi-Fi маршрутизатори) TL-WDR3500	https://www.tp-link.com/uk-ua/support/emulator/
116.	TP-LINK	(Wi-Fi маршрутизатори) Archer C6 TL-WR941ND	https://www.tp-link.com/uk-ua/support/emulator/
117.	TP-LINK	(Wi-Fi маршрутизатори) Archer A6 TL-WR843ND	https://www.tp-link.com/uk-ua/support/emulator/
118.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR843N	https://www.tp-link.com/uk-ua/support/emulator/
119.	TP-LINK	(Wi-Fi маршрутизатори) Archer C60 TL-WR743ND	https://www.tp-link.com/uk-ua/support/emulator/
120.	TP-LINK	(Wi-Fi маршрутизатори) Archer A5	https://www.tp-link.com/uk-ua/support/emulator/
121.	TP-LINK	(Wi-Fi маршрутизатори) Archer C20	https://www.tp-link.com/uk-ua/support/emulator/
122.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR940N	https://www.tp-link.com/uk-ua/support/emulator/
123.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR840N	https://www.tp-link.com/uk-ua/support/emulator/
124.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR720N	https://www.tp-link.com/uk-ua/support/emulator/
125.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR710N	https://www.tp-link.com/uk-ua/support/emulator/
126.	TP-LINK	(Wi-Fi маршрутизатори) TL-WR702N	https://www.tp-link.com/uk-ua/support/emulator/
127.	Tenda	FH456	https://www.tendacn.com/simulator/default.html
128.	Tenda	RX27 Pro	https://www.tendacn.com/simulator/default.html
129.	Tenda	AC10	https://www.tendacn.com/simulator/default.html
130.	Tenda	RX2 Pro	https://www.tendacn.com/simulator/default.html
131.	Tenda	V12	https://www.tendacn.com/simulator/default.html
132.	Tenda	W20E	https://www.tendacn.com/simulator/default.html
133.	Tenda	W18E	https://www.tendacn.com/simulator/default.html
134.	Tenda	RX3	https://www.tendacn.com/simulator/default.html
135.	Tenda	F6	https://www.tendacn.com/simulator/default.html
136.	Tenda	AC8 v2.0	https://www.tendacn.com/simulator/default.html
137.	Tenda	AC23	https://www.tendacn.com/simulator/default.html
138.	Tenda	AC19	https://www.tendacn.com/simulator/default.html
139.	Tenda	AC21	https://www.tendacn.com/simulator/default.html
140.	Tenda	v300	https://www.tendacn.com/simulator/default.html
141.	Tenda	F3 v3	https://www.tendacn.com/simulator/default.html
142.	Cisco linksys	E1000	https://ui.linksys.com/ExpertFamily/
143.	Cisco linksys	E1200	https://ui.linksys.com/ExpertFamily/
144.	Cisco linksys	E1500	https://ui.linksys.com/ExpertFamily/
145.	Cisco linksys	E1550	https://ui.linksys.com/ExpertFamily/
146.	Cisco linksys	E1700	https://ui.linksys.com/ExpertFamily/
147.	Cisco linksys	E2000	https://ui.linksys.com/ExpertFamily/
148.	Cisco linksys	E2100L	https://ui.linksys.com/ExpertFamily/
149.	Cisco linksys	E2500	https://ui.linksys.com/ExpertFamily/
150.	Cisco linksys	E3000	https://ui.linksys.com/ExpertFamily/
151.	Cisco linksys	E3200	https://ui.linksys.com/ExpertFamily/
152.	Cisco linksys	E4200	https://ui.linksys.com/ExpertFamily/
153.	Cisco linksys	E5350	https://ui.linksys.com/ExpertFamily/
154.	Cisco linksys	E5400	https://ui.linksys.com/ExpertFamily/
155.	Cisco linksys	E7350	https://ui.linksys.com/ExpertFamily/
156.	Cisco linksys	E8350	https://ui.linksys.com/ExpertFamily/
157.	Cisco linksys	E8400	https://ui.linksys.com/ExpertFamily/
158.	Cisco linksys	E900	https://ui.linksys.com/ExpertFamily/
159.	Cisco linksys	E9450_AH	https://ui.linksys.com/ExpertFamily/
160.	Cisco linksys	E9450_US	https://ui.linksys.com/ExpertFamily/
161.	Cisco linksys	X1000	https://ui.linksys.com/ExpertFamily/
162.	Cisco linksys	X2000	https://ui.linksys.com/ExpertFamily/

№	БРЕНД	НАЗВА ПРИСТРОЮ	ГІПЕРПОСИЛАННЯ
163.	Cisco linksys	X3000	https://ui.linksys.com/ExpertFamily/
164.	Cisco linksys	X3500	https://ui.linksys.com/ExpertFamily/
165.	Cisco linksys	X6200	https://ui.linksys.com/ExpertFamily/
166.	Cisco linksys	XAC1200	https://ui.linksys.com/ExpertFamily/
167.	Cisco linksys	XAC1900	https://ui.linksys.com/ExpertFamily/
168.	Cisco linksys	EA2700	https://ui.linksys.com/SmartWi-FiFamilyRouters/
169.	Cisco linksys	EA3500	https://ui.linksys.com/SmartWi-FiFamilyRouters/
170.	Cisco linksys	EA4500	https://ui.linksys.com/SmartWi-FiFamilyRouters/
171.	Cisco linksys	EA6100	https://ui.linksys.com/SmartWi-FiFamilyRouters/
172.	Cisco linksys	EA6200	https://ui.linksys.com/SmartWi-FiFamilyRouters/
173.	Cisco linksys	EA6300	https://ui.linksys.com/SmartWi-FiFamilyRouters/
174.	Cisco linksys	EA6350	https://ui.linksys.com/SmartWi-FiFamilyRouters/
175.	Cisco linksys	EA6400	https://ui.linksys.com/SmartWi-FiFamilyRouters/
176.	Cisco linksys	EA6500	https://ui.linksys.com/SmartWi-FiFamilyRouters/
177.	Cisco linksys	EA6700	https://ui.linksys.com/SmartWi-FiFamilyRouters/
178.	Cisco linksys	EA6900	https://ui.linksys.com/SmartWi-FiFamilyRouters/
179.	Cisco linksys	EA7500	https://ui.linksys.com/SmartWi-FiFamilyRouters/
180.	Cisco linksys	EA8300	https://ui.linksys.com/SmartWi-FiFamilyRouters/
181.	Cisco linksys	EA8500	https://ui.linksys.com/SmartWi-FiFamilyRouters/
182.	Cisco linksys	EA9200	https://ui.linksys.com/SmartWi-FiFamilyRouters/
183.	Cisco linksys	EA9300	https://ui.linksys.com/SmartWi-FiFamilyRouters/
184.	Cisco linksys	EA9500	https://ui.linksys.com/SmartWi-FiFamilyRouters/
185.	Cisco linksys	FGW3000	https://ui.linksys.com/SmartWi-FiFamilyRouters/
186.	Cisco linksys	WRT1200AC	https://ui.linksys.com/SmartWi-FiFamilyRouters/
187.	Cisco linksys	WRT1900AC	https://ui.linksys.com/SmartWi-FiFamilyRouters/
188.	Cisco linksys	WRT3200ACM	https://ui.linksys.com/SmartWi-FiFamilyRouters/
189.	Cisco linksys	WRT32X	https://ui.linksys.com/SmartWi-FiFamilyRouters/
190.	TOTOLINK	A7000R	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
191.	TOTOLINK	A3100R	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
192.	TOTOLINK	A810R	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
193.	TOTOLINK	A3000RU	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
194.	TOTOLINK	A950RG	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
195.	TOTOLINK	A800R	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
196.	TOTOLINK	A1004	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
197.	TOTOLINK	A2004NS	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
198.	TOTOLINK	A6004NS	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
199.	TOTOLINK	A5004NS	https://www.totolink.net/home/news/me_name/menu_listtpl/support/id/41.html
200.	MERCUSYS	MW325R	https://www.mercusys.com/simulator/mw325rv2-en/web/common/Index.htm
201.	MERCUSYS	AC12G	https://www.mercusys.com/simulator/emulator_AC12G(EU)3.0_router/emulator_EU_router/index.html
202.	MERCUSYS	AC1200G	https://www.mercusys.com/simulator/AC1200G(RU)1.0_Emulator/index.html
203.	MERCUSYS	AC10	https://www.mercusys.com/simulator/ac10-router/index.html
204.	MERCUSYS	MR30G	https://www.mercusys.com/simulator/mr30g_eu_ap/index.html
205.	MERCUSYS	MR62X	https://www.mercusys.com/simulator/ipf-mr62x-emulator-eu&us/index.html
206.	MERCUSYS	MR50G	https://www.mercusys.com/simulator/mr50g_eu_router/
207.	MERCUSYS	MR80X	https://www.mercusys.com/simulator/mr80xv3-emulator/index.html
208.	MERCUSYS	MW301R	https://www.mercusys.com/simulator/emulator_EU_router/index.html

ЗАВДАННЯ

Визначити свій індивідуальний варіант завдання - відповідно до списку наданого у курсі “Комп’ютерні мережі” (дистанційне навчання ЦНТУ https://moodle.kntu.kr.ua/course/view.php?id=1035)

ЧАСТИНА 1. Використовуючи **програмні мережні емулятори** та видані варіанти емуляторів виконайте наступні завдання:

1. Увійдіть в систему за допомогою логіна і пароля за замовчуванням (зазвичай admin і порожній пароль або admin).

2. Налаштуйте новий пароль для адміністратора роутера у форматі «[прізвище виконавця латиницею]_[номер варіанту]».

3. Змініть IP-адресу роутера на 192.168.1.[номер варіанту].

4. Змініть SSID (ім'я мережі) на «[назва роутера]_[прізвище виконавця латиницею]».

5. Змініть пароль мережі на дату виконання роботи (8 цифр у форматі 27.08.2024 -> 27082024).

6. Налаштувати DHCP-сервер для отримання IP-адрес клієнтами мережі: Створіть новий пул IP-адрес для клієнтів (192.168.1.100-192.168.1.[номер варіанту]).

7. Налаштувати перенаправлення портів для доступу до локального пристрою з адресою 192.168.1.[номер варіанту].

8. Налаштувати гостьову мережу без пароля з лімітом на скачування згідно [номеру варіанту].

При виникненні питань що-до можливості реалізації зверніться до асистента курсу.

ЗВЕРНІТЬ УВАГУ! В деяких онлайн емуляторах не зберігаються налаштування то по виконанню кожного завдання окремо рекомендовано робити підтверджуючі скриншоти з вікном де вносилися зміни в налаштування обладнання.

ЧАСТИНА 2. Використовуючи наявні **маршрутизатори** фізично розташовані в локальній мережі кафедри КБПЗ ЦНТУ та виданий варіант маршрутизатора (уточнити у асистента курсу), проведіть підключення до обладнання за допомогою даних отриманих даних (IP, Login, Password) та повторіть завдання частини 1.

ОФОРМЛЕННЯ ЗВІТУ

У звіт лабораторної роботи помістити:

– Завдання л/роботи відповідно до виданого варіанту.

– Покрокові матеріали що повністю підтверджують виконання л/роботи (текст, таблиці, скриншоти, та інші матеріали для підтвердження виконання л/роботи).

– Короткі змістовні відповіді на л/роботи.

Лабораторну роботу оформляти по загальноприйнятій формі (ДСТУ) та аналогічно до інших предметів кафедри КБПЗ ЦНТУ.

КОНТРОЛЬНІ ЗАПИТАННЯ

Основні поняття та терміни

1. Що таке маршрутизатор і яка його основна функція в мережі?
2. Які відмінності між комутатором (switch) і маршрутизатором?
3. Що таке таблиця маршрутизації і яку інформацію вона містить?
4. Що таке статична і динамічна маршрутизація? Наведіть приклади.
5. Які протоколи динамічної маршрутизації ви знаєте? Які їх основні характеристики?

Налаштування маршрутизатора

6. Як здійснюється підключення до маршрутизатора для його налаштування? Які є способи?
7. Які основні команди використовуються для налаштування IP-адреси інтерфейсу маршрутизатора?

8. Що таке шлюз за замовчуванням і як його налаштувати на маршрутизаторі?

9. Як перевірити, що маршрутизатор успішно встановив зв’язок з іншими пристроями в мережі?

10. Як додати статичний маршрут в таблицю маршрутизації? Яка команда для цього використовується?

Протоколи маршрутизації

11. Які особливості протоколу RIP (Routing Information Protocol)?

12. Що таке OSPF (Open Shortest Path First) і як він працює?

13. Як відбувається налаштування протоколу RIP на маршрутизаторі?

14. У чому полягають переваги та недоліки використання протоколів динамічної маршрутизації?

Безпека та управління

15. Які механізми безпеки можна використовувати для захисту маршрутизатора?

16. Як створити і застосувати список доступу (ACL) на маршрутизаторі для обмеження доступу до певних мережевих ресурсів?

17. Як налаштувати віддалений доступ до маршрутизатора за допомогою SSH або Telnet?

18. Які методи можна використовувати для моніторингу та управління продуктивністю маршрутизатора?

Практичні аспекти

19. Що таке NAT (Network Address Translation) і як його налаштувати на маршрутизаторі?

20. Які можливості надає функція QoS (Quality of Service) і як вона впливає на маршрутизацію?

Лабораторна робота №3

ТЕМА: РОБОТА ТА АНАЛІЗ МЕРЕЖНОЇ КЛІЄНТ-СЕРВЕРНОЇ ВЗАЄМОДІЇ

МЕТА: Отримати практичні навики роботи з сокетами TCP/IP та використання мережних аналізаторів

ЗНАТИ: Основи мережної взаємодії та мови програмування високого рівня

ТЕОРЕТИЧНІ ВІДОМОСТІ

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором):

– https://uk.wikipedia.org/wiki/Клієнт-серверна_архітектура.

– https://uk.wikipedia.org/wiki/Архітектурні_шаблони_програмного_забезпечення.

– https://uk.wikipedia.org/wiki/Аналізатор_трафіку.

– https://wiki.wireshark.org/CaptureFilters.

– https://uk.wikipedia.org/wiki/Wireshark.

– https://uk.wikipedia.org/wiki/Tcpdump.

– Дистрибутив «Wireshark»: https://www.wireshark.org.

– https://uk.wikipedia.org/wiki/Telnet.

Приклади роботи з клієнт- серверною взаємодією сокетів на різних мовах (C#, Python, Java):

– https://www.youtube.com/watch?v=ypQgE5rBCpA&ab_channel=CodingWorld

– https://www.youtube.com/watch?v=3QiPPX-KeSc&ab_channel=TechWithTim

–https://www.youtube.com/watch?v=JNzfG7XMYSg&t=1s&ab_channel=KindsonTheTechPro

– https://www.youtube.com/watch?v=-xKgxqG411c&ab_channel=ThenisH

ЗАВДАННЯ

ЧАСТИНА 1.

Використовуючи мову програмування високого рівня (на вибір студента), розробити клієнт-серверне ПЗ з наступним функціоналом.

1. Серверне ПЗ (рис. 1), логіка роботи.

При запуску серверного ПЗ, на екран виводяться дані для підключення клієнта: IP адрес; порт сервера. Сервер переходить в режим очікування підключення клієнтів з виведенням поточної інформації на екран (моніторинг). Сервер аналізує список підключених клієнтів із заданою періодичністю і виводить його на екран, в противному випадку виводить повідомлення, що підключених клієнтів немає.

При підключенні клієнта сервер виводить його дані - IP-адреса, порт, поточний стан (On-line) і очікує інформаційний пакет даних. При отриманні інформаційного пакета даних проводить його читання та виведення результату на екран.

2. Клієнтське ПЗ (рис. 2), логіка роботи.

Клієнт підключається до сервера і відправляє із заданою періодичністю інформаційне повідомлення про свою присутність (стані On-line). По запиту користувача за один раз відправляє «інформаційний пакет даних» до сервера.

Визначити свій індивідуальний варіант завдання можна відповідно до списку наданого у курсі “Комп’ютерні мережі” (дистанційне навчання ЦНТУ https://moodle.kntu.kr.ua/course/view.php?id=1035)

Звернувшись до таблиці 3.1 з індивідуальним варіантом завдання отримуємо унікальний набір полів 1-5 (інформаційний пакет даних).

На рисунку 1,б наведено приклад сформованого інформаційного пакету даних:

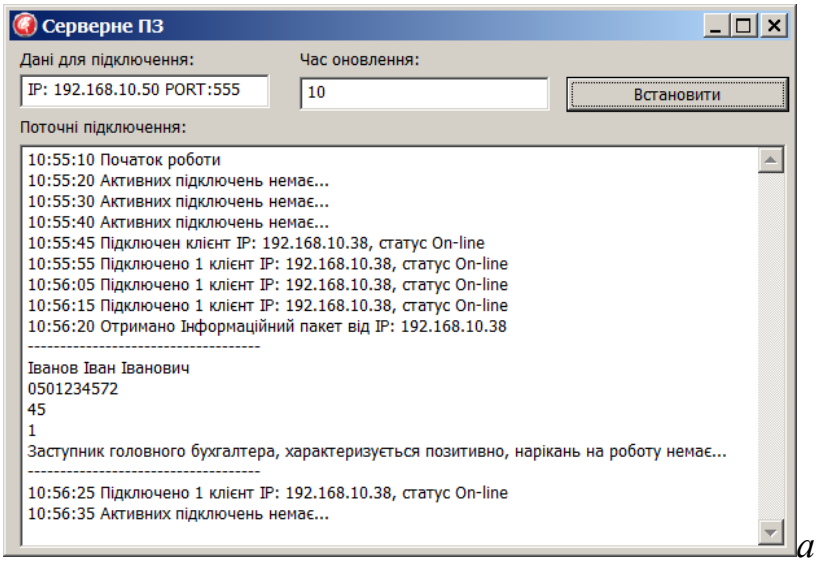
– Поле 1 (строковий тип): П.І.Б;

– Поле 2 (строковий тип): Номер телефону;

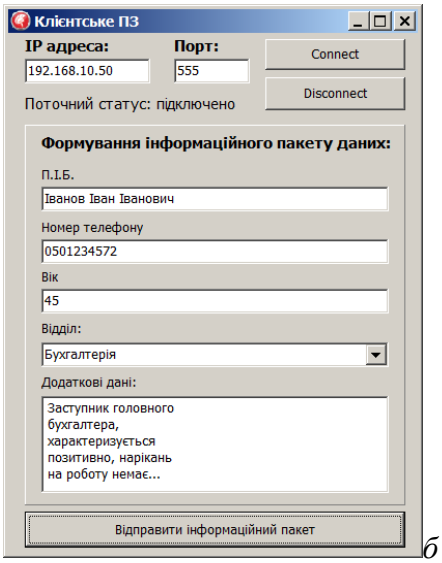
– Поле 3 (числовий тип): Вік;

– Поле 4 (перерахунковий тип) Відділ: (1)Бухгалтерія, (2)Менеджери, (3)Закупівлі, (4)IT-підтримка;

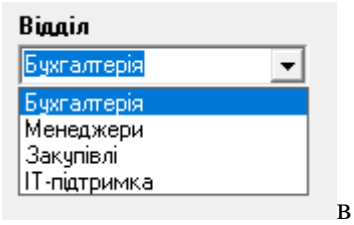
– Поле 5 (Неформатований текст обмеженого розміру до 255 символів): Додаткові дані.



а



б



в

Рисунок 1 – Приклад роботи клієнт-серверного ПЗ: а – сервер, б – клієнт, в – приклад реалізації перерахункового типу у клієнтському ПЗ

Таблиця 3.1 Список варіантів інформаційного пакету даних

№ вар	Поле 1	Поле 2	Поле 3	Поле 4	Поле 5
1.	ФІО (строковий тип)	Контактний номер (строковий тип)	Дата народження (числовий тип)	Технології (перерахунковий тип: (1) Java, (2) Python, (3) C++, (4) JavaScript)	Додаткова інформація (неформатований текст максимально 255 символів)

2.	Ім'я користувача (строковий тип)	Службовий номер (строковий тип)	Стаж (числовий тип)	Метод тестування (перерахунковий тип: (1) Unit-тестування, (2) Інтеграційне, (3) Регресійне, (4) Навантажувальне)	Коментарі щодо тестування (неформатований текст максимально 255 символів)
3.	Повне ім'я (строковий тип)	Телефонний номер (строковий тип)	Роки (числовий тип)	Модель розробки (перерахунковий тип: (1) Agile, (2) Waterfall, (3) Scrum, (4) Kanban)	Примітки (неформатований текст максимально 255 символів)
4.	Прізвище (строковий тип)	Телефон (строковий тип)	Вік (числовий тип)	Спеціалізація (перерахунковий тип: (1) Мережі, (2) Бази даних, (3) Кібербезпека, (4) Хмарні обчислення)	Опис (неформатований текст максимально 255 символів)
5.	ФІО (строковий тип)	Контактний номер (строковий тип)	Дата народження (числовий тип)	Технології (перерахунковий тип: (1) Java, (2) Python, (3) C++, (4) JavaScript)	Додаткова інформація (неформатований текст максимально 255 символів)
6.	П.І.Б (строковий тип)	Номер телефону (строковий тип)	Вік (числовий тип)	Роль у проекті (перерахунковий тип: (1) Розробник, (2) Тестувальник, (3) Архітектор, (4) Бізнес-аналітик)	Додаткові дані (неформатований текст максимально 255 символів)
7.	ФІО (строковий тип)	Контактний номер (строковий тип)	Дата народження (числовий тип)	Технології (перерахунковий тип: (1) Java, (2) Python, (3) C++, (4))	Додаткова інформація (неформатований текст максимально 255 символів)
8.	П.І.Б (строковий тип)	Номер телефону (строковий тип)	Вік (числовий тип)	Роль у проекті (перерахунковий тип: (1) Розробник, (2) Тестувальник, (3) Архітектор, (4) Бізнес-аналітик)	Додаткові дані (неформатований текст максимально 255 символів)
9.	Ім'я користувача (строковий тип)	Службовий номер (строковий тип)	Стаж (числовий тип)	Метод тестування (перерахунковий тип: (1) Unit-тестування, (2) Інтеграційне, (3) Регресійне, (4) Навантажувальне)	Коментарі щодо тестування (неформатований текст максимально 255 символів)
10.	Повне ім'я (строковий тип)	Телефонний номер (строковий тип)	Роки (числовий тип)	Модель розробки (перерахунковий тип: (1) Agile, (2) Waterfall, (3) Scrum, (4) Kanban)	Примітки (неформатований текст максимально 255 символів)
11.	П.І.Б (строковий тип)	Номер телефону (строковий тип)	Вік (числовий тип)	Роль у проекті (перерахунковий тип: (1) Розробник, (2) Тестувальник, (3) Архітектор, (4) Бізнес-аналітик)	Додаткові дані (неформатований текст максимально 255 символів)
12.	Ім'я (строковий тип)	Мобільний номер (строковий тип)	Рік народження (числовий тип)	Область знань (перерахунковий тип: (1) Фронтенд, (2) Бекенд, (3) ДевОпс, (4) Безпека)	Коментарі (неформатований текст максимально 255 символів)

13.	Ім'я (строковий тип)	Мобільний номер (строковий тип)	Рік народження (числовий тип)	Область знань (перерахунковий тип: (1) Фронтенд, (2) Бекенд, (3) ДевОпс, (4) Безпека)	Коментарі (неформатований текст максимально 255 символів)
14.	Прізвище (строковий тип)	Телефон (строковий тип)	Вік (числовий тип)	Спеціалізація (перерахунковий тип: (1) Мережі, (2) Бази даних, (3) Кібербезпека, (4) Хмарні обчислення)	Опис (неформатований текст максимально 255 символів)
15.	Ім'я (строковий тип)	Мобільний номер (строковий тип)	Рік народження (числовий тип)	Область знань (перерахунковий тип: (1) Фронтенд, (2) Бекенд, (3) ДевОпс, (4) Безпека)	Коментарі (неформатований текст максимально 255 символів)
16.	ФІО (строковий тип)	Контактний номер (строковий тип)	Дата народження (числовий тип)	Технології (перерахунковий тип: (1) Java, (2) Python, (3) C++, (4) JavaScript)	Додаткова інформація (неформатований текст максимально 255 символів)
17.	Ім'я (строковий тип)	Мобільний номер (строковий тип)	Рік народження (числовий тип)	Область знань (перерахунковий тип: (1) Фронтенд, (2) Бекенд, (3) ДевОпс, (4) Безпека)	Коментарі (неформатований текст максимально 255 символів)
18.	Програміст (строковий тип)	Контактний телефон (строковий тип)	Кількість проєктів (числовий тип)	Операційна система (перерахунковий тип: (1) Windows, (2) Linux, (3) macOS, (4) Unix)	Деталі про операційні системи (неформатований текст максимально 255 символів)
19.	Ім'я користувача (строковий тип)	Службовий номер (строковий тип)	Стаж (числовий тип)	Метод тестування (перерахунковий тип: (1) Unit-тестування, (2) Інтеграційне, (3) Регресійне, (4) Навантажувальне)	Коментарі щодо тестування (неформатований текст максимально 255 символів)
20.	П.І.Б (строковий тип)	Номер телефону (строковий тип)	Вік (числовий тип)	Роль у проекті (перерахунковий тип: (1) Розробник, (2) Тестувальник, (3) Архітектор, (4) Бізнес-аналітик)	Додаткові дані (неформатований текст максимально 255 символів)
21.	Програміст (строковий тип)	Контактний телефон (строковий тип)	Кількість проєктів (числовий тип)	Операційна система (перерахунковий тип: (1) Windows, (2) Linux, (3) macOS, (4) Unix)	Деталі про операційні системи (неформатований текст максимально 255 символів)
22.	ФІО (строковий тип)	Контактний номер (строковий тип)	Дата народження (числовий тип)	Технології (перерахунковий тип: (1) Java, (2) Python, (3) C++, (4) JavaScript)	Додаткова інформація (неформатований текст максимально 255 символів)

23.	Програміст (строковий тип)	Контактний телефон (строковий тип)	Кількість проєктів (числовий тип)	Операційна система (перерахунковий тип: (1) Windows, (2) Linux, (3) macOS, (4) Unix)	Деталі про операційні системи (неформатований текст максимально 255 символів)
24.	Прізвище (строковий тип)	Телефон (строковий тип)	Вік (числовий тип)	Спеціалізація (перерахунковий тип: (1) Мережі, (2) Бази даних, (3) Кібербезпека, (4) Хмарні обчислення)	Опис (неформатований текст максимально 255 символів)
25.	Ім'я (строковий тип)	Мобільний номер (строковий тип)	Рік народження (числовий тип)	Область знань (перерахунковий тип: (1) Фронтенд, (2) Бекенд, (3) ДевОпс, (4) Безпека)	Коментарі (неформатований текст максимально 255 символів)
26.	Повне ім'я (строковий тип)	Телефонний номер (строковий тип)	Роки (числовий тип)	Модель розробки (перерахунковий тип: (1) Agile, (2) Waterfall, (3) Scrum, (4) Kanban)	Примітки (неформатований текст максимально 255 символів)
27.	Повне ім'я (строковий тип)	Телефонний номер (строковий тип)	Роки (числовий тип)	Модель розробки (перерахунковий тип: (1) Agile, (2) Waterfall, (3) Scrum, (4) Kanban)	Примітки (неформатований текст максимально 255 символів)
28.	Прізвище (строковий тип)	Телефон (строковий тип)	Вік (числовий тип)	Спеціалізація (перерахунковий тип: (1) Мережі, (2) Бази даних, (3) Кібербезпека, (4) Хмарні обчислення)	Опис (неформатований текст максимально 255 символів)
29.	Програміст (строковий тип)	Контактний телефон (строковий тип)	Кількість проєктів (числовий тип)	Операційна система (перерахунковий тип: (1) Windows, (2) Linux, (3) macOS, (4) Unix)	Деталі про операційні системи (неформатований текст максимально 255 символів)
30.	Ім'я (строковий тип)	Мобільний номер (строковий тип)	Рік народження (числовий тип)	Область знань (перерахунковий тип: (1) Фронтенд, (2) Бекенд, (3) ДевОпс, (4) Безпека)	Коментарі (неформатований текст максимально 255 символів)
31.	Прізвище (строковий тип)	Телефон (строковий тип)	Вік (числовий тип)	Спеціалізація (перерахунковий тип: (1) Мережі, (2) Бази даних, (3) Кібербезпека, (4) Хмарні обчислення)	Опис (неформатований текст максимально 255 символів)
32.	Прізвище (строковий тип)	Телефон (строковий тип)	Вік (числовий тип)	Спеціалізація (перерахунковий тип: (1) Мережі, (2) Бази даних, (3) Кібербезпека, (4) Хмарні обчислення)	Опис (неформатований текст максимально 255 символів)
33.	Повне ім'я (строковий тип)	Телефонний номер (строковий тип)	Роки (числовий тип)	Модель розробки (перерахунковий тип: (1) Agile, (2) Waterfall, (3) Scrum, (4) Kanban)	Примітки (неформатований текст максимально 255 символів)

34.	ФІО (строковий тип)	Контактний номер (строковий тип)	Дата народження (числовий тип)	Технології (перерахунковий тип: (1) Java, (2) Python, (3) C++, (4) JavaScript)	Додаткова інформація (неформатований текст максимально 255 символів)
35.	Повне ім'я (строковий тип)	Телефонний номер (строковий тип)	Роки (числовий тип)	Модель розробки (перерахунковий тип: (1) Agile, (2) Waterfall, (3) Scrum, (4) Kanban)	Примітки (неформатований текст максимально 255 символів)
36.	Повне ім'я (строковий тип)	Телефонний номер (строковий тип)	Роки (числовий тип)	Модель розробки (перерахунковий тип: (1) Agile, (2) Waterfall, (3) Scrum, (4) Kanban)	Примітки (неформатований текст максимально 255 символів)
37.	Ім'я (строковий тип)	Мобільний номер (строковий тип)	Рік народження (числовий тип)	Область знань (перерахунковий тип: (1) Фронтенд, (2) Бекенд, (3) ДевОпс, (4) Безпека)	Коментарі (неформатований текст максимально 255 символів)
38.	Ім'я користувача (строковий тип)	Службовий номер (строковий тип)	Стаж (числовий тип)	Метод тестування (перерахунковий тип: (1) Unit-тестування, (2) Інтеграційне, (3) Регресійне, (4) Навантажувальне)	Коментарі щодо тестування (неформатований текст максимально 255 символів)
39.	Ім'я (строковий тип)	Мобільний номер (строковий тип)	Рік народження (числовий тип)	Область знань (перерахунковий тип: (1) Фронтенд, (2) Бекенд, (3) ДевОпс, (4) Безпека)	Коментарі (неформатований текст максимально 255 символів)
40.	Ім'я (строковий тип)	Мобільний номер (строковий тип)	Рік народження (числовий тип)	Область знань (перерахунковий тип: (1) Фронтенд, (2) Бекенд, (3) ДевОпс, (4) Безпека)	Коментарі (неформатований текст максимально 255 символів)

ЧАСТИНА 2.

Використовуючи вільно обраний мережний аналізатор (рекомендується Wireshark) провести сканування локальної мережі під час роботи розробленого клієнт-серверного ПЗ (ЧАСТИНА 1).

Проаналізувати трафік локальної мережі, створити фільтри які дозволяють он-лайн переглядати наступне:

1. Всі пакети які передаються розробленим ПЗ під час клієнт-серверного обміну даними.

2. Тільки «Інформаційний пакет даних» відправлений клієнтським ПЗ по запиту користувача з представленням даних що передаються.

ЧАСТИНА 3.

За допомогою telnet підключитись до порту розробленого серверного ПЗ, наприклад (рисунок 1,а):

```
telnet 192.168.10.50 555
```

Спробувати подати команди клієнтської програми вручну.

ОФОРМЛЕННЯ ЗВІТУ

У звіт лабораторної роботи помістити:

– Завдання л/роботи відповідно до виданого варіанту.

– Покрокові матеріали що повністю підтверджують виконання л/роботи (текст, таблиці, принтскріни, та інші матеріали для підтвердження виконання л/роботи).

– Короткі змістовні відповіді на л/роботи.

Лабораторну роботу оформляти по загальноприйнятій формі (ДСТУ) та аналогічно до інших предметів кафедри КБПЗ ЦНТУ.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. На даний час яка є домінуюча концепція у створенні розподілених мережних систем?
2. Наведіть приклади використання архітектурного шаблону «Модель-вид-контролер»?
3. Наведіть приклади використання архітектурного шаблону «Клієнт-серверна архітектура»?
4. Наведіть приклади використання архітектурного шаблону «Три-ярусна архітектура»?
5. Наведіть приклади використання архітектурного шаблону «Сервісно-орієнтована архітектура»?
6. Якими способами може здійснюватись перехоплення трафіку?
7. Аналіз трафіку, що пройшов через мережний аналізатор, дозволяє?

8. Наведіть найпоширеніші існуючі мережні аналізатори?

9. Які переваги використання мережного аналізатора Wireshark від існуючих аналогів?

10. За допомогою яких засобів можна знизити загрозу мережного аналізу трафіку?

Лабораторна робота №4

ТЕМА: ДОСЛІДЖЕННЯ МЕРЕЖЕВИХ ТОПОЛОГІЙ З ВИКОРИСТАННЯМ CISCO PACKET TRACER ТА GNS3

МЕТА: Практичне використання і застосування знань архітектури і топології локальної мережі, побудова мереж за допомогою програм моделювання

ЗНАТИ: Основи мережної взаємодії, будову обраної мережі.

ТЕОРЕТИЧНІ ВІДОМОСТІ

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором):

– https://uk.wikipedia.org/wiki/Кільцева_топологія_мережі.

– https://uk.wikipedia.org/wiki/Топологія_мереж.

– https://uk.wikipedia.org/wiki/Шина_(топологія).

– https://uk.wikipedia.org/wiki/Зірка_(топологія).

– https://www.cisco.com/c/uk_ua/index.html.

– https://www.netacad.com/courses/packet-tracer.

– https://www.udemy.com/course/ccna-gns3-packet-tracer-virl-physical-equipment-pass-exam.

– https://www.classcentral.com/classroom/youtube-gns3-start-here-if-you-are-new-to-gns3-80203.

– https://www.packettracernetwork.com/download/download-packet-tracer.html.

– https://www.gns3.com/.

– https://en.wikipedia.org/wiki/Graphical_Network_Simulator-3.

ЗАВДАННЯ

Частина 1. Надати звіт, що містить наступну інформацію:

Завдання 1.1. **Проаналізувати** рисунок 1.1 та на його основі використовуючи додані додаткові файли у форматі .drawio («Загальний план поверхів», «Network Research Center») **сформувати** докладну локальну мережу кафедри «Кібербезпеки та програмного забезпечення» Центральноукраїнського національного університету з зазначенням кожного ПК та шляхів доступу до Глобальної мережі Інтернет.

При побудові карти мережі для звіту використовувати сайт рисування діаграм он-лайн «https://app.diagrams.net/» нотація Cisco 19.

При створенні використовувати розділ Cisco 19 нотація з підрозділами:

– Cisco 19/Endpoint Client and Device Icon.

– Cisco 19/ Routing WAN.

– Cisco 19/LAN Switching.

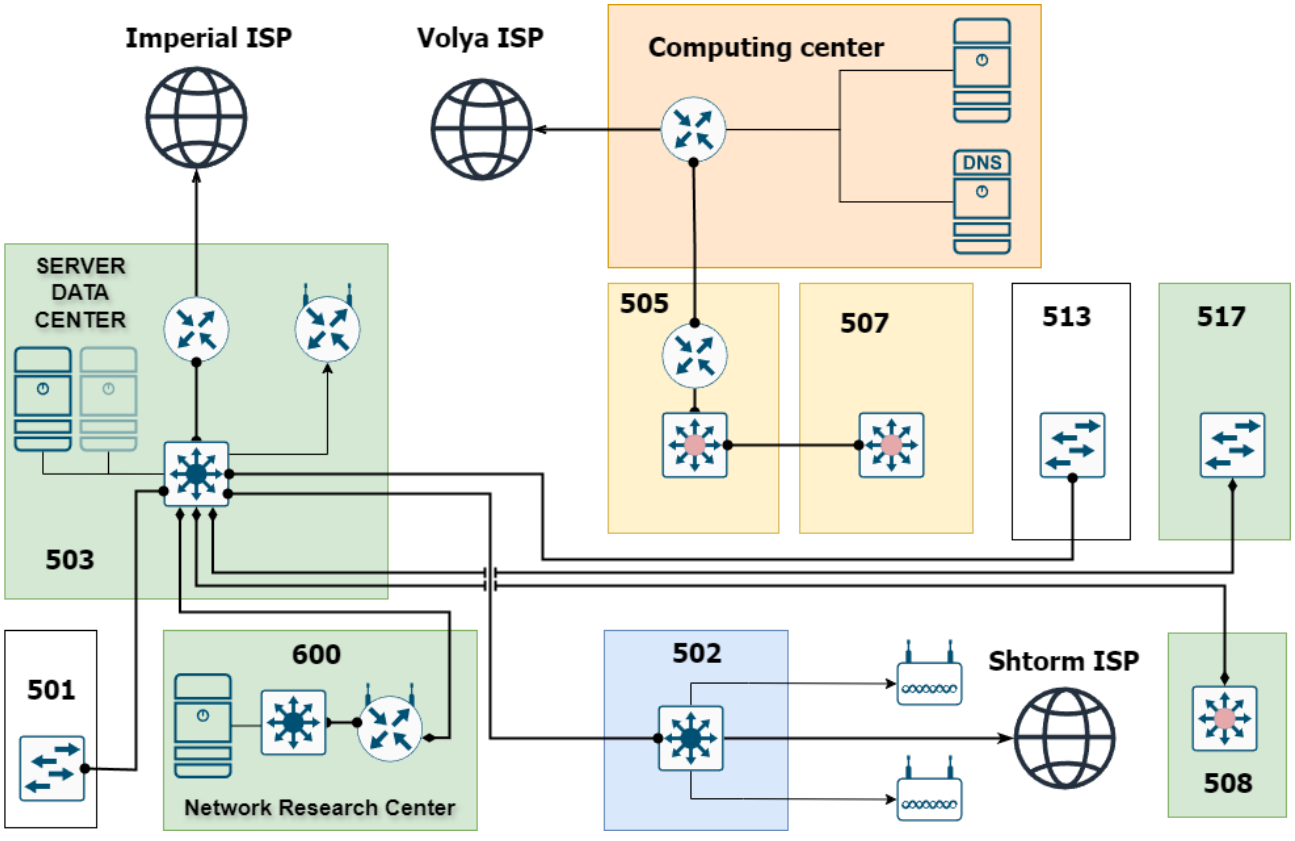


Рисунок 4.1 – Приклад спрощеної локальної мережі

Завдання 1.2. Представити приклади мереж з топологією – **шина, зірка, кільце, дерево**. Використовувати сайт рисування діаграм он-лайн «https://app.diagrams.net/» нотація Cisco 19.

Можливо використання інших засобів крім diagrams.net (погоджувати з асистентом курсу).

Частина 2.

Завдання 2.1 На основі виконаного завдання (частина 1 завдання 1.1) використовуючи ПЗ Cisco packet tracer розробити та показати роботу мережі кафедри «Кібербезпеки та програмного забезпечення» Центральноукраїнського національного університету.

Необхідно задати ip-адреси, маски підмережі і шлюзи за замовчуванням для всіх вузлів мережі, щоб забезпечити коректну доставку Echo-запитів і Echo-відповідей (команда ping). Як результат забезпечити можливість проводити ping запити у сформованій мережі. Сформувати звіт з л/р, що містить повну інформацію про локальну мережу кафедри.

Частина 3.

Завдання 3.1. На основі виконаного завдання (частина 1 завдання 1.1) та розробленої схеми (частина 2 завдання 2.1) використовуючи ПЗ GNS3 (Graphical Network Simulator-3) також показати роботу мережі КБПЗ ЦНТУ з демонстрацією роботи на апаратних пристроях кафедри та сервісів мережі що неможливо реалізувати у ПЗ Cisco packet tracer.

ОФОРМЛЕННЯ ЗВІТУ

У звіт лабораторної роботи помістити:

– Завдання л/роботи.

– Покрокові матеріали що повністю підтверджують виконання л/роботи (текст, таблиці, принтскріни, та інші матеріали для підтвердження виконання л/роботи).

– Короткі змістовні відповіді на л/роботи.

Лабораторну роботу оформляти по загальноприйнятій формі (ДСТУ) та аналогічно до інших предметів кафедри КБПЗ ЦНТУ.

КОНТРОЛЬНІ ЗАПИТАННЯ

ТОПОЛОГІЇ МЕРЕЖ

1. Що таке мережна топологія, і чому вона важлива при проектуванні мереж?

2. Які властивості базової топології комп'ютерної мережі шина (bus)?

3. Які властивості базової топології комп'ютерної мережі зірка (star)?

4. Які властивості базової топології комп'ютерної мережі кільце (ring)?

5. Які властивості похідної топології комп'ютерної мережі подвійне кільце?

6. Які властивості похідної топології комп'ютерної мережі сотова топологія?

7. Які властивості похідної топології комп'ютерної мережі решітка?

8. Які властивості похідної топології комп'ютерної мережі дерево?

РИСУВАННЯ ДІАГРАМ ЛОКАЛЬНОЇ МЕРЕЖІ В DRAW.IO

9. Які переваги та недоліки використання draw.io для проектування мереж у порівнянні з іншими програмами?

10. Яка мета використання нотацій Cisco 19 Endpoint Client and Device Icon, Cisco 19/ Routing WAN, Cisco 19/LAN Switching при створенні діаграм мереж в draw.io?

11. Як правильно використати нотації Cisco для зображення маршрутизаторів, комутаторів і кінцевих пристроїв у draw.io?

ВИКОРИСТАННЯ ПРОГРАМ МОДЕЛЮВАННЯ МЕРЕЖІ CISCO PACKET TRACER

12. Які основні можливості надає Cisco Packet Tracer для моделювання мереж?

13. Як у Cisco Packet Tracer створити мережу, що включає маршрутизатор, комутатор і кілька кінцевих пристроїв?

14. Яким чином можна перевірити з'єднання між пристроями в Cisco Packet Tracer? Які інструменти для цього використовуються?

15. Як у Cisco Packet Tracer налаштувати статичні маршрути?

16. Які інструменти Cisco Packet Tracer дозволяють моделювати роботу DHCP-сервера?

ВИКОРИСТАННЯ ПРОГРАМ МОДЕЛЮВАННЯ МЕРЕЖІ GNS3 (GRAPHICAL NETWORK SIMULATOR-3)

17. Що таке GNS3 і які його основні переваги перед іншими мережними симуляторами?

18. Як у GNS3 можна налаштувати з'єднання між віртуальною мережею і реальним обладнанням?

19. Як у GNS3 використовувати Docker-контейнери для моделювання спеціалізованих мережевих сервісів?

20. Які кроки потрібно виконати для налаштування з'єднання між двома віртуальними машинами в різних підмережах у GNS3?

Лабораторна робота №5

ТЕМА: ВИВЧЕННЯ СЕРВІСІВ ЛОКАЛЬНОЇ МЕРЕЖІ

МЕТА: Практичне використання і застосування знань архітектури і топології локальної мережі, побудова мереж за допомогою програм моделювання

ЗНАТИ: Основи мережної взаємодії, будову обраної мережі.

ТЕОРЕТИЧНІ ВІДОМОСТІ

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором):

– https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

– https://www.fortinet.com/resources/cyberglossary/what-is-dns

– https://en.wikipedia.org/wiki/Web_service

– https://en.wikipedia.org/wiki/Mailbox_provider

– https://www.fortinet.com/resources/cyberglossary/file-transfer-protocol-ftp-meaning

– https://en.wikipedia.org/wiki/VLAN

ЗАВДАННЯ

Частина 1.

Визначити свій індивідуальний варіант завдання можна відповідно до списку наданого у курсі “Комп’ютерні мережі” (дистанційне навчання ЦНТУ https://moodle.kntu.kr.ua/course/view.php?id=1035).

Використовуючи ПЗ Cisco packet tracer розробити та показати роботу локальної мережі на основі рисунку 5.1. Звернувшись до таблиці 5.1 з

індивідуальним варіантом завдання отримуємо унікальний набір полів для налаштування локальної мережі.

НЕОБХІДНО НАЛАШТУВАТИ НАСТУПНІ СЕРВІСИ.

1. DHCP (Dynamic Host Configuration Protocol) це мережевий протокол, який автоматично призначає IP-адреси всім кінцевим пристроям. Він дозволяє пристроям отримувати ці налаштування автоматично без необхідності ручного введення. На рисунку 5.1 зображено сервером з написом «Server-PT DHCP».

Приклад запису конфігурації «DHCP (dhcp-range)» **2 стовпчик, таблиця 5.1**

dhcp-range=92.34.140.139, 92.34.140.166, 255.255.255.0

dhcp-range це параметр, який вказує діапазон IP-адрес, що буде видаватися DHCP-сервером. 92.34.140.139, 92.34.140.166: це діапазон IP-адрес, які DHCP-сервер може призначати клієнтам.

У наведеному прикладі адреси будуть призначатися в межах від 139 до 166, тобто 166-139=максимум 27 машин. 255.255.255.0 це маска підмережі, яка вказує, що використовувана підмережа має 256 адрес (класична підмережа з 24 бітами для мережевої частини і 8 бітами для адреси хоста). Це означає, що клієнти в мережі можуть отримувати IP-адреси з цього діапазону, і всі пристрої будуть в одній підмережі.

2. HTTP-сервер (Hypertext Transfer Protocol Server) – сервер, який приймає, обробляє та відповідає на запити, надіслані через протокол HTTP. Основне його призначення — надавати веб-контент (наприклад, веб-сторінки, файли) користувачам або іншим пристроям у мережі. Приклад роботи – браузер відправляє запит наприклад, "GET /index.html". HTTP-сервер знаходить файл index.html і відправляє його назад клієнту. Браузер отримує файл і відображає його користувачу.

Приклад запису конфігурації «WEB server» **3 стовпчик, таблиця 5.1**

HTTP SERVER: 92.34.140.138, TEXT (index.html):2732

HTTP SERVER – IP адреса WEB сервера, у прикладі це 92.34.140.138.

TEXT (index.html):2732 – який текст виводиться якщо відкрити главний файл сайту index.html, у прикладі це текст 2732.

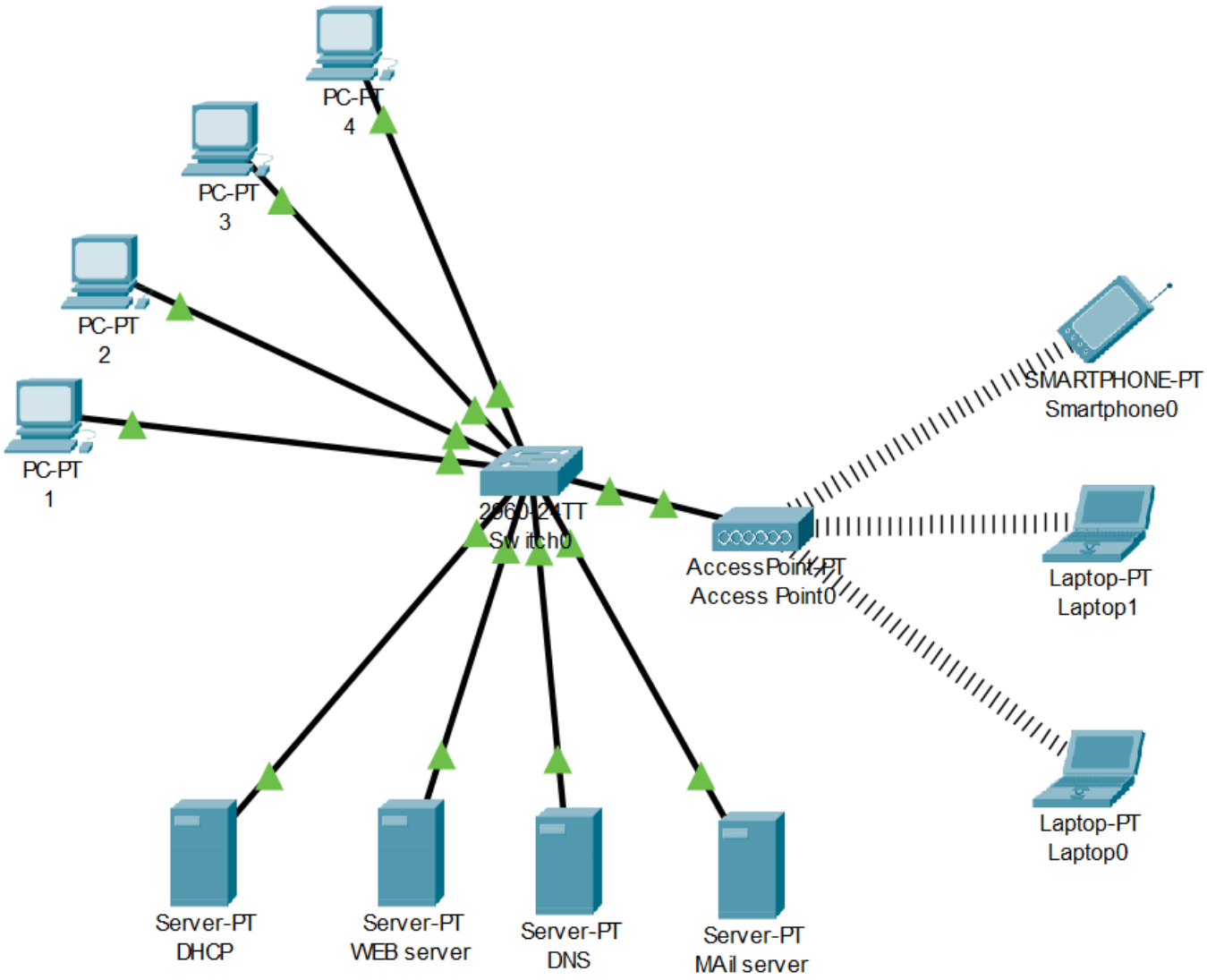


Рисунок 5.1 – Приклад локальної мережі з залученням мережних сервісів

3. DNS (Domain Name System) – система доменних імен, яка перетворює зрозумілі для людей доменні імена (наприклад,

www.example.com) у машинні IP-адреси (192.0.2.1), які використовуються для доступу до інтернет-ресурсів. «A record» – пов'язує доменне ім'я з IPv4-адресою.

Приклад запису конфігурації «DNS (A record)» **4 стовпчик, таблиця 5.1**

www.WEB107.com. IN A 92.34.140.138

www.WEB107.com – доменне ім'я, яке запитує користувач (вебсайт або ресурс). Точка в кінці завершує введення доменного ім'я.

IN A – індикатор того, що цей DNS-запис є A record і він використовує IPv4 адресу.

92.34.140.138 – IPv4-адреса сервера, на якому розміщений вебсайт. Всі запити до "www.WEB107.com" будуть перенаправлятися на сервер за цією IP-адресою.

4. Email (Electronic Mail) – метод обміну повідомленнями через інтернет або інші комп'ютерні мережі, що дозволяє користувачам надсилати та отримувати текстові повідомлення, а також вкладення (файли, зображення, документи) у цифровій формі. SMTP і POP3 — це два основні протоколи, які використовуються для надсилання та отримання електронної пошти. SMTP (Simple Mail Transfer Protocol) – протокол для надсилання електронної пошти. POP3 (Post Office Protocol version 3) – протокол для отримання електронної пошти.

Приклад запису конфігурації «EMAIL SMTP, POP3 (A record)» **5 стовпчик, таблиця 5.1**

lecturemail200.com. IN A 92.34.140.137

Формат запису A record (по аналогії з 3 пунктом DNS).

5. FTP (File Transfer Protocol) – мережевий протокол, який використовується для передачі файлів між комп'ютерами через мережу (зазвичай через інтернет). FTP дозволяє як завантажувати файли на сервер (upload), так і завантажувати файли з сервера (download).

Приклад запису конфігурації «FTP (authentication data)» 6 стовпчик, таблиця 5.1

User: Person1 Pass: 125 Permission: RW

User: Person1 – логін користувача

Pass:125 – пароль користувача

Permission: RW – дозволи користувача формату RWDNL це набір прав доступу для FTP (або інших файлових систем), які визначають, що користувач може робити з файлами або каталогами. Ось що означає кожна з цих літер:

R (Read) — Читання: користувач може переглядати або завантажувати файли.

W (Write) — Запис: користувач може створювати нові файли або змінювати існуючі.

D (Delete) — Видалення: користувач може видаляти файли або каталоги.

N (Rename) — Перейменування: користувач може змінювати назви файлів або каталогів.

L (List) — Список: користувач може переглядати список файлів і каталогів.

Таблиця 5.1 Список варіантів інформаційного пакету даних

№	DHCP (dhcp-range)	WEB server	DNS (A record)	EMAIL SMTP, POP3 (A record)	FTP (authentication data)
41.	dhcp-range= 92.34.140.139, 92.34.140.166, 255.255.255.0	HTTP SERVER: 92.34.140.138, TEXT (index.html):2732	www.WEB107.com. IN A 92.34.140.138	lecturemail200.com. IN A 92.34.140.137	User: Person1 Pass:125 Permission:RW

42.	dhcp-range= 66.185.150.84, 66.185.150.126, 255.255.255.0	HTTP SERVER: 66.185.150.83, TEXT (index.html):9602	www.WEB300.com. IN A 66.185.150.83	lecturemail084.com. IN A 66.185.150.82	User: Person2 Pass:136 Permission:RL
43.	dhcp-range= 149.102.230.78, 149.102.230.103, 255.255.255.0	HTTP SERVER: 149.102.230.77, TEXT (index.html):9801	www.WEB147.com. IN A 149.102.230.77	lecturemail465.com. IN A 149.102.230.76	User: Person3 Pass:022 Permission:RL
44.	dhcp-range= 35.220.154.99, 35.220.154.172, 255.255.255.0	HTTP SERVER: 35.220.154.98, TEXT (index.html):2593	www.WEB587.com. IN A 35.220.154.98	lecturemail533.com. IN A 35.220.154.97	User: Person4 Pass:585 Permission:W
45.	dhcp-range= 162.187.37.14, 162.187.37.92, 255.255.255.0	HTTP SERVER: 162.187.37.13, TEXT (index.html):6351	www.WEB940.com. IN A 162.187.37.13	lecturemail250.com. IN A 162.187.37.12	User: Person5 Pass:737 Permission:RWDNL
46.	dhcp-range= 80.195.24.94, 80.195.24.165, 255.255.255.0	HTTP SERVER: 80.195.24.93, TEXT (index.html):7103	www.WEB321.com. IN A 80.195.24.93	lecturemail690.com. IN A 80.195.24.92	User: Person6 Pass:417 Permission:NR
47.	dhcp-range= 126.184.19.61, 126.184.19.76, 255.255.255.0	HTTP SERVER: 126.184.19.60, TEXT (index.html):7471	www.WEB170.com. IN A 126.184.19.60	lecturemail303.com. IN A 126.184.19.59	User: Person7 Pass:232 Permission:LWDN
48.	dhcp-range= 101.207.157.68, 101.207.157.100, 255.255.255.0	HTTP SERVER: 101.207.157.67, TEXT (index.html):1740	www.WEB118.com. IN A 101.207.157.67	lecturemail127.com. IN A 101.207.157.66	User: Person8 Pass:055 Permission:DLRW
49.	dhcp-range= 125.124.253.100, 125.124.253.191, 255.255.255.0	HTTP SERVER: 125.124.253.99, TEXT (index.html):9664	www.WEB866.com. IN A 125.124.253.99	lecturemail210.com. IN A 125.124.253.98	User: Person9 Pass:596 Permission:WNL
50.	dhcp-range= 169.54.110.75, 169.54.110.89, 255.255.255.0	HTTP SERVER: 169.54.110.74, TEXT (index.html):8295	www.WEB169.com. IN A 169.54.110.74	lecturemail666.com. IN A 169.54.110.73	User: Person10 Pass:082 Permission:NRWD
51.	dhcp-range= 50.60.199.126, 50.60.199.173, 255.255.255.0	HTTP SERVER: 50.60.199.125, TEXT (index.html):9098	www.WEB682.com. IN A 50.60.199.125	lecturemail767.com. IN A 50.60.199.124	User: Person11 Pass:464 Permission:NLWR
52.	dhcp-range= 171.6.175.25, 171.6.175.81, 255.255.255.0	HTTP SERVER: 171.6.175.24, TEXT (index.html):9975	www.WEB785.com. IN A 171.6.175.24	lecturemail856.com. IN A 171.6.175.23	User: Person12 Pass:472 Permission:LWDN
53.	dhcp-range= 220.57.14.117, 220.57.14.214, 255.255.255.0	HTTP SERVER: 220.57.14.116, TEXT (index.html):2639	www.WEB555.com. IN A 220.57.14.116	lecturemail359.com. IN A 220.57.14.115	User: Person13 Pass:655 Permission:WNRD
54.	dhcp-range= 22.167.219.43, 22.167.219.120, 255.255.255.0	HTTP SERVER: 22.167.219.42, TEXT (index.html):3381	www.WEB392.com. IN A 22.167.219.42	lecturemail938.com. IN A 22.167.219.41	User: Person14 Pass:096 Permission:NDLR
55.	dhcp-range= 228.152.76.144, 228.152.76.190, 255.255.255.0	HTTP SERVER: 228.152.76.143, TEXT (index.html):4344	www.WEB010.com. IN A 228.152.76.143	lecturemail117.com. IN A 228.152.76.142	User: Person15 Pass:235 Permission:RW
56.	dhcp-range= 241.44.59.123, 241.44.59.223, 255.255.255.0	HTTP SERVER: 241.44.59.122, TEXT (index.html):4492	www.WEB035.com. IN A 241.44.59.122	lecturemail615.com. IN A 241.44.59.121	User: Person16 Pass:060 Permission:NWRLD

57.	dhcp-range= 127.107.84.145, 127.107.84.168, 255.255.255.0	HTTP SERVER: 127.107.84.144, TEXT (index.html):6928	www.WEB604.com. IN A 127.107.84.144	lecturemail035.com. IN A 127.107.84.143	User: Person17 Pass:137 Permission:R
58.	dhcp-range= 225.92.8.128, 225.92.8.228, 255.255.255.0	HTTP SERVER: 225.92.8.127, TEXT (index.html):2274	www.WEB567.com. IN A 225.92.8.127	lecturemail624.com. IN A 225.92.8.126	User: Person18 Pass:324 Permission:D
59.	dhcp-range= 59.223.97.79, 59.223.97.90, 255.255.255.0	HTTP SERVER: 59.223.97.78, TEXT (index.html):8397	www.WEB998.com. IN A 59.223.97.78	lecturemail549.com. IN A 59.223.97.77	User: Person19 Pass:085 Permission:WLD
60.	dhcp-range= 248.240.79.101, 248.240.79.150, 255.255.255.0	HTTP SERVER: 248.240.79.100, TEXT (index.html):2445	www.WEB405.com. IN A 248.240.79.100	lecturemail829.com. IN A 248.240.79.99	User: Person20 Pass:575 Permission:DWLR
61.	dhcp-range= 248.23.225.128, 248.23.225.135, 255.255.255.0	HTTP SERVER: 248.23.225.127, TEXT (index.html):6522	www.WEB108.com. IN A 248.23.225.127	lecturemail165.com. IN A 248.23.225.126	User: Person21 Pass:289 Permission:LWD
62.	dhcp-range= 152.218.82.60, 152.218.82.71, 255.255.255.0	HTTP SERVER: 152.218.82.59, TEXT (index.html):1065	www.WEB597.com. IN A 152.218.82.59	lecturemail173.com. IN A 152.218.82.58	User: Person22 Pass:486 Permission:N
63.	dhcp-range= 144.78.230.114, 144.78.230.175, 255.255.255.0	HTTP SERVER: 144.78.230.113, TEXT (index.html):3056	www.WEB699.com. IN A 144.78.230.113	lecturemail293.com. IN A 144.78.230.112	User: Person23 Pass:778 Permission:RLN
64.	dhcp-range= 110.198.161.83, 110.198.161.142, 255.255.255.0	HTTP SERVER: 110.198.161.82, TEXT (index.html):5716	www.WEB406.com. IN A 110.198.161.82	lecturemail555.com. IN A 110.198.161.81	User: Person24 Pass:083 Permission:D
65.	dhcp-range= 127.191.109.104, 127.191.109.161, 255.255.255.0	HTTP SERVER: 127.191.109.103, TEXT (index.html):6293	www.WEB700.com. IN A 127.191.109.103	lecturemail097.com. IN A 127.191.109.102	User: Person25 Pass:584 Permission:WL
66.	dhcp-range= 136.128.86.13, 136.128.86.29, 255.255.255.0	HTTP SERVER: 136.128.86.12, TEXT (index.html):7110	www.WEB839.com. IN A 136.128.86.12	lecturemail816.com. IN A 136.128.86.11	User: Person26 Pass:820 Permission:RN
67.	dhcp-range= 34.130.179.124, 34.130.179.215, 255.255.255.0	HTTP SERVER: 34.130.179.123, TEXT (index.html):2806	www.WEB597.com. IN A 34.130.179.123	lecturemail736.com. IN A 34.130.179.122	User: Person27 Pass:362 Permission:DNRL
68.	dhcp-range= 166.19.91.57, 166.19.91.112, 255.255.255.0	HTTP SERVER: 166.19.91.56, TEXT (index.html):5158	www.WEB933.com. IN A 166.19.91.56	lecturemail404.com. IN A 166.19.91.55	User: Person28 Pass:579 Permission:D
69.	dhcp-range= 224.195.67.11, 224.195.67.57, 255.255.255.0	HTTP SERVER: 224.195.67.10, TEXT (index.html):5365	www.WEB636.com. IN A 224.195.67.10	lecturemail486.com. IN A 224.195.67.9	User: Person29 Pass:590 Permission:LNDRW
70.	dhcp-range= 85.116.141.40, 85.116.141.86, 255.255.255.0	HTTP SERVER: 85.116.141.39, TEXT (index.html):7440	www.WEB615.com. IN A 85.116.141.39	lecturemail723.com. IN A 85.116.141.38	User: Person30 Pass:626 Permission:LR
71.	dhcp-range= 78.12.47.106, 78.12.47.152, 255.255.255.0	HTTP SERVER: 78.12.47.105, TEXT (index.html):3546	www.WEB191.com. IN A 78.12.47.105	lecturemail912.com. IN A 78.12.47.104	User: Person31 Pass:483 Permission:LNR

72.	dhcp-range= 34.245.24.66, 34.245.24.106, 255.255.255.0	HTTP SERVER: 34.245.24.65, TEXT (index.html):4305	www.WEB577.com. IN A 34.245.24.65	lecturemail229.com. IN A 34.245.24.64	User: Person32 Pass:614 Permission:N
73.	dhcp-range= 170.26.201.79, 170.26.201.113, 255.255.255.0	HTTP SERVER: 170.26.201.78, TEXT (index.html):4103	www.WEB596.com. IN A 170.26.201.78	lecturemail267.com. IN A 170.26.201.77	User: Person33 Pass:981 Permission:LR
74.	dhcp-range= 193.191.137.117, 193.191.137.124, 255.255.255.0	HTTP SERVER: 193.191.137.116, TEXT (index.html):7302	www.WEB256.com. IN A 193.191.137.116	lecturemail022.com. IN A 193.191.137.115	User: Person34 Pass:471 Permission:WDLRN
75.	dhcp-range= 219.226.252.149, 219.226.252.179, 255.255.255.0	HTTP SERVER: 219.226.252.148, TEXT (index.html):7434	www.WEB095.com. IN A 219.226.252.148	lecturemail712.com. IN A 219.226.252.147	User: Person35 Pass:247 Permission:WRNDL
76.	dhcp-range= 40.4.16.50, 40.4.16.101, 255.255.255.0	HTTP SERVER: 40.4.16.49, TEXT (index.html):7545	www.WEB540.com. IN A 40.4.16.49	lecturemail012.com. IN A 40.4.16.48	User: Person36 Pass:325 Permission:DL
77.	dhcp-range= 10.27.163.29, 10.27.163.113, 255.255.255.0	HTTP SERVER: 10.27.163.28, TEXT (index.html):6648	www.WEB794.com. IN A 10.27.163.28	lecturemail728.com. IN A 10.27.163.27	User: Person37 Pass:378 Permission:WL
78.	dhcp-range= 26.82.246.132, 26.82.246.138, 255.255.255.0	HTTP SERVER: 26.82.246.131, TEXT (index.html):8016	www.WEB570.com. IN A 26.82.246.131	lecturemail702.com. IN A 26.82.246.130	User: Person38 Pass:235 Permission:N
79.	dhcp-range= 10.48.59.44, 10.48.59.105, 255.255.255.0	HTTP SERVER: 10.48.59.43, TEXT (index.html):4747	www.WEB160.com. IN A 10.48.59.43	lecturemail365.com. IN A 10.48.59.42	User: Person39 Pass:848 Permission:DR
80.	dhcp-range= 123.192.101.24, 123.192.101.104, 255.255.255.0	HTTP SERVER: 123.192.101.23, TEXT (index.html):6971	www.WEB794.com. IN A 123.192.101.23	lecturemail819.com. IN A 123.192.101.22	User: Person40 Pass:575 Permission:LRW

ОФОРМЛЕННЯ ЗВІТУ

У звіт лабораторної роботи помістити:

– Завдання л/роботи відповідно до виданого варіанту.

– Покрокові матеріали що повністю підтверджують виконання л/роботи (текст, таблиці, принтскріни, та інші матеріали для підтвердження виконання л/роботи).

– Короткі змістовні відповіді на л/роботи.

Лабораторну роботу оформляти по загальноприйнятій формі (ДСТУ) та аналогічно до інших предметів кафедри КБПЗ ЦНТУ.

КОНТРОЛЬНІ ЗАПИТАННЯ

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

1. Що таке DHCP і яка його основна функція?
2. Які основні компоненти DHCP-системи?

DNS (DOMAIN NAME SYSTEM)

3. Що таке DNS і як він працює?
4. Як налаштувати DNS-записи для веб-сайту?
5. Що таке кешування DNS і як воно працює?
6. Які інструменти можна використовувати для діагностики проблем з DNS?

WEB (WEB SERVICES)

7. Що таке веб-сервер і які його основні функції?
8. Які популярні програмні рішення - веб-сервери використовуються у практиці?
9. Що таке SSL/TLS і як їх використовують для захисту веб-сайтів?

MAIL (EMAIL SERVICES)

10. Що таке поштовий сервер і які його основні функції?
11. Які основні компоненти поштового сервера?
12. Як налаштувати базовий поштовий сервер для надсилання та отримання листів?

FTP (FILE TRANSFER PROTOCOL)

13. Що таке FTP/TFTP і які його основні функції?
14. Які основні режими роботи FTP?
15. Як налаштувати базовий FTP-сервер для передачі файлів?
16. Які методи аутентифікації використовуються в FTP?

VLAN (VIRTUAL LOCAL AREA NETWORK)

17. Що таке VLAN і як він використовується в мережах?
18. Як налаштувати VLAN?
19. Як VLAN впливає на безпеку мережі?

Лабораторна робота №6

ТЕМА: ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК ТА ПАРАМЕТРІВ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI

МЕТА: Отримати практичні навички в налаштуванні, моніторингу та оцінці параметрів мережі, а також зрозуміти вплив різних факторів на продуктивність та стабільність з'єднання в умовах реальної експлуатації.

ЗНАТИ: Основи комп'ютерних мереж, IP-адресації, мережевих протоколів та основи мережевої безпеки.

ТЕОРЕТИЧНІ ВІДОМОСТІ

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором):

– Що впливає на роботу Wi-Fi мережі? https://help.bcm.net.ua/shho-vplyvaye-na-robotu-wi-fi-merezhi/.

– Wireless local area networks https://www.ieee802.org/11/.

– The Evolution of Wi-Fi Technology and Standards https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements.

– The Evolution of Wi-Fi Technology and Standards https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/.

– Wi-Fi 7 Technology Trends https://www.anritsu.com/en-US/test-measurement/technologies/wlan/wlan6gfeatures/wifi7?click-from-wifiparent.

– 802.11 Wireless Standards Explained https://community.fs.com/article/802-11-standards-explained.html.

– DBm https://uk.wikipedia.org/wiki/DBm/.

– What is a Wi-Fi Heat Map https://www.netally.com/wifi-solutions/what-is-a-wifi-heatmap-and-how-do-i-read-one/.

– Як прискорити Wi-Fi. https://nsoft-s.com/ua/mychatarticles/1546-yak-pryskoryry-miy-wifi.html

ЗАВДАННЯ

ЧАСТИНА 1. ОЦІНКА ЯКОСТІ ТА ЗОН ПОКРИТТЯ WI-FI

Використовуючи доданий у 4 л/р план поверхів (рис. 6.1) **оцінити якість та зону покриття всіх наявних Wi-Fi мереж на 5 поверсі**.

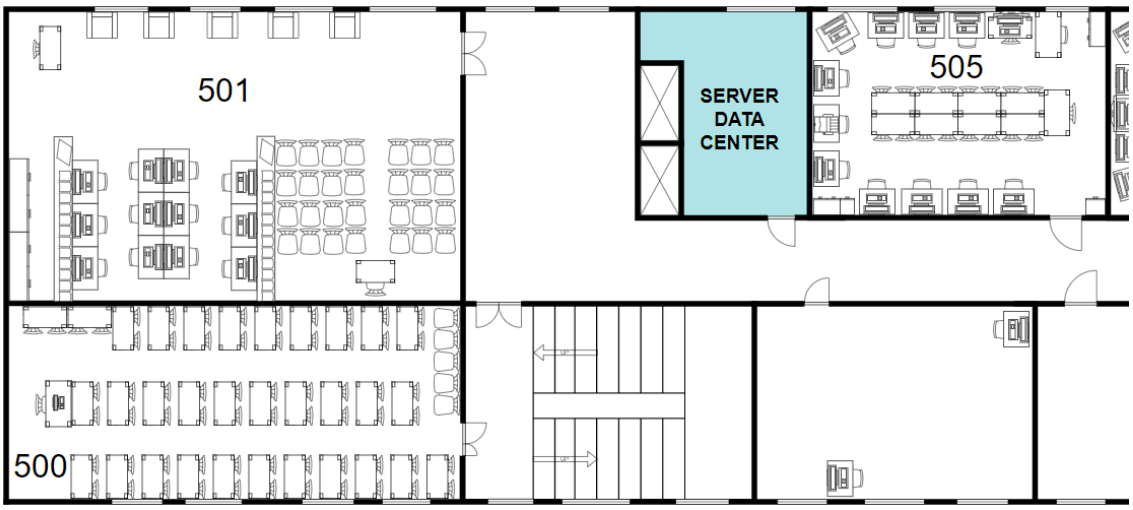


Рисунок 6.1 – Частковий план поверху

За допомогою наступних засобів:

1.1. Стандартна утиліта ping.exe протокол ICMP (Internet Control Message Protocol). Результат у вигляді **мілісекунд** довільним чином нанести на план поверху.

1.2. Signal Strength. Результат у вигляді **dBM** довільним чином нанести на план поверху. Можливо використання інших аналогічних програм.

Посилання:

https://play.google.com/store/apps/details?id=com.cls.networkwidget

1.3. Wi-Fi Surveyor. Результат у **вигляді теплової карти Wi-fi** (Wi-Fi Heat Map) на плані поверху (рис. 6.2). Можливо використання інших аналогічних програм.

Посилання: https://github.com/ecoAPM/WiFiSurveyor.

ЗВЕРНІТЬ УВАГУ! При виникненні питань що-до варіантів реалізації зверніться до асистента курсу. Дві однакові теплові карти Wi-fi не приймаються!

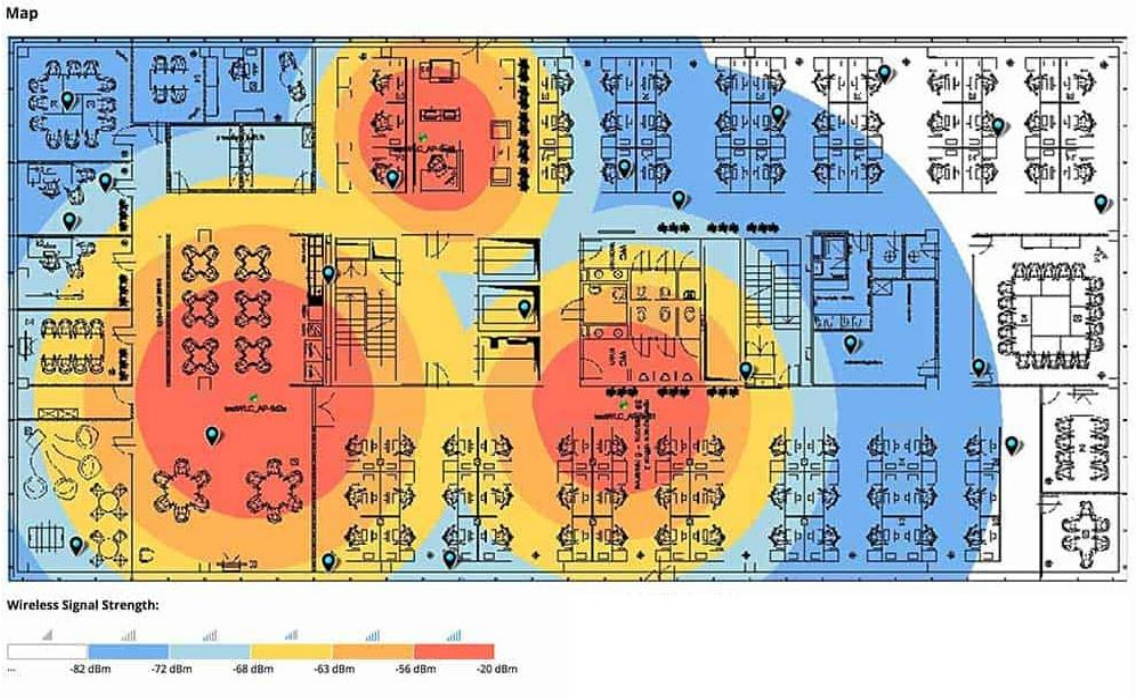


Рисунок 6.2 – Приклад спрощеної теплової карти Wi-fi

ЧАСТИНА 2. WI-FI ІНТЕРФЕРЕНЦІЯ.

Використовуючи обладнання центру мережевих досліджень каб.600б дослідити Wi-fi інтерференцію на частоті 2.4 Ггц.

2.1 Підготовка

Wi-Fi інтерференція це сигнал, що випромінюється іншими пристроями (як у межах вашої мережі Wi-Fi, так і поза нею) на тому ж або сусідньому каналі, на якому працює ваш пристрій.

Налаштувати 7 Wi-fi мереж на 6 канал частота 2,4 Ггц (рис.6.3) та вимкнути джерела інтерференції, залишити тільки одну еталонну мережу.

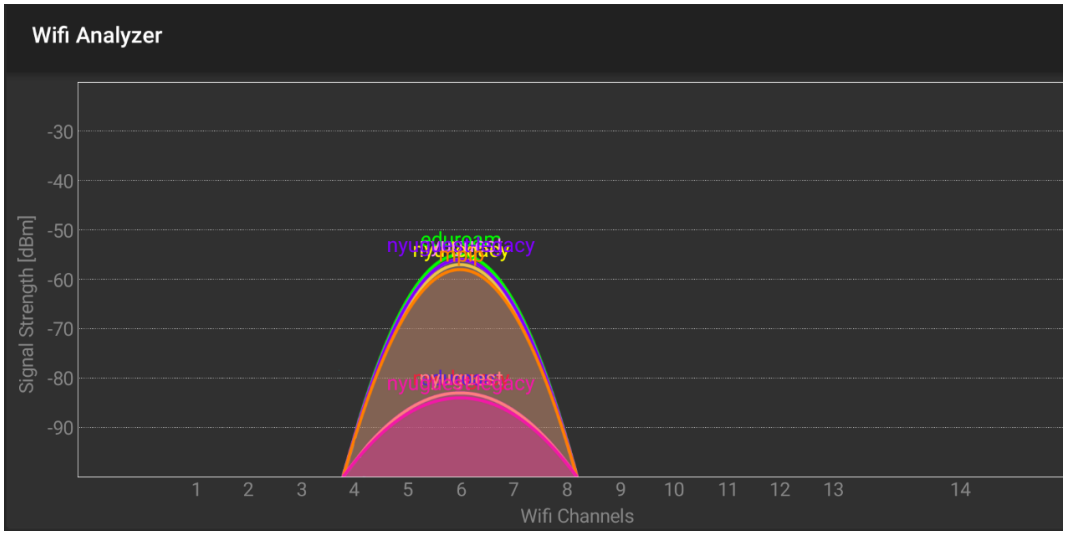


Рисунок 6.3 – Приклад налаштування точок доступу на 6 канал, частота 2,4 Ггц

Визначитись чим проводить заміри параметрів. Можливі різні варіанти, пропонується використовувати iPerf3/Ping.

Замір швидкості через iPerf3

Посилання: https://help.bcm.net.ua/iperf3/

Download Iperf3

Посилання: https://iperf.fr/iperf-download.php

Public iPerf3 servers

Посилання: https://iperf.fr/iperf-servers.php

2.2 Проведення вимірювань.

Провести первинний аналіз якості сигналу Wi-Fi у приміщенні на єдиної основі еталонного пристрою, зафіксувати показники сили сигналу та інтенсивність мережі на каналах (рис.6.4). Активувати джерела інтерференції. Повторити вимірювання сили сигналу Wi-Fi, звертаючи увагу на зміни (рис.6.5).

2.3 Аналіз результатів та пропозиції щодо мінімізації інтерференції.

Порівняти результати вимірювань до та після активації джерел інтерференції.

У звіт лабораторної роботи помістити:

– Завдання л/роботи.

– Покрокові матеріали що повністю підтверджують виконання л/роботи (текст, таблиці, принтскріни, та інші матеріали для підтвердження виконання л/роботи).

– Проаналізувати дані та оцінити якість зв’язку залежно від вибору каналу та наявності чи відсутності джерел інтерференції.

– Надати пропозиції щодо оптимізації точок доступу Wi-Fi мережі на основі отриманих даних.

– Короткі змістовні відповіді на л/роботи.

Лабораторну роботу оформляти по загальноприйнятій формі (ДСТУ) та аналогічно до інших предметів кафедри КБПЗ ЦНТУ.

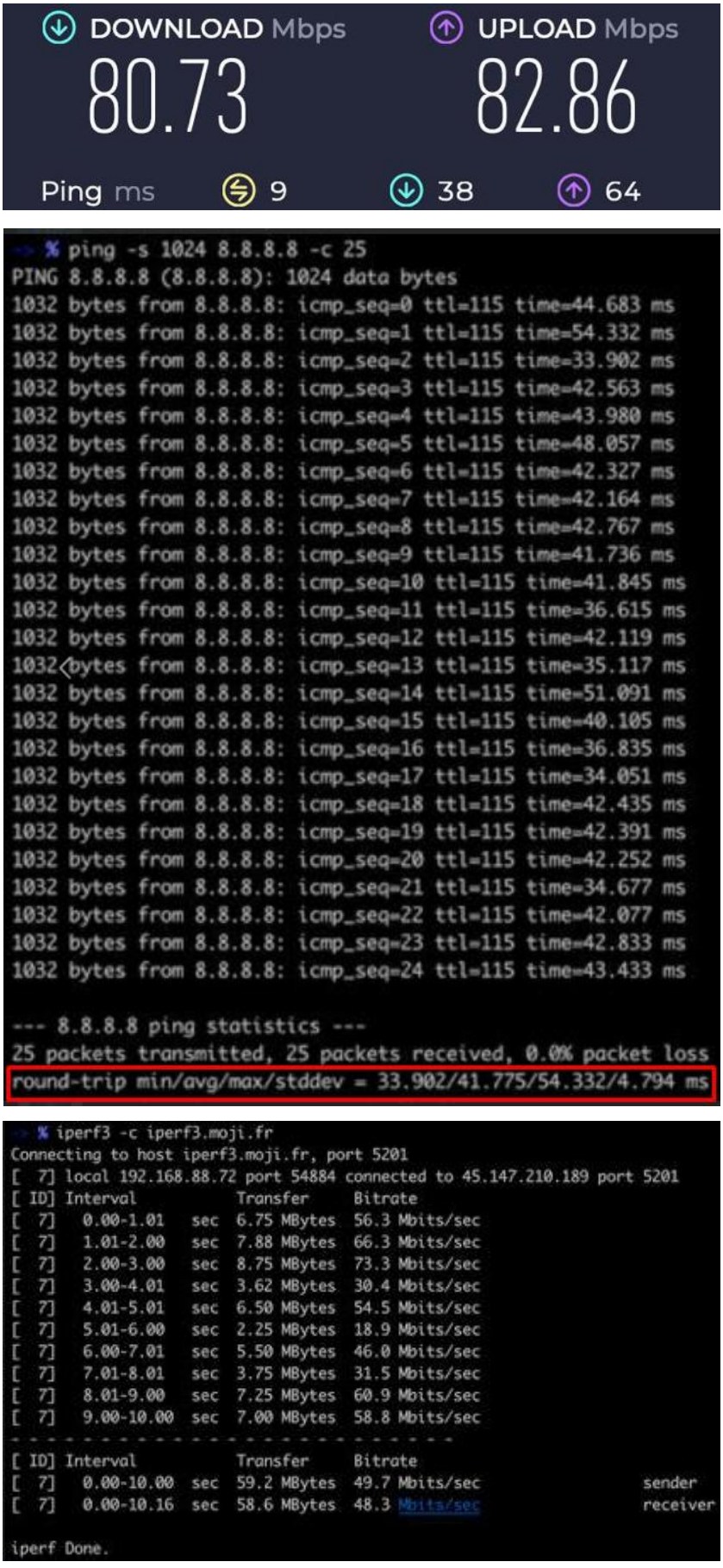
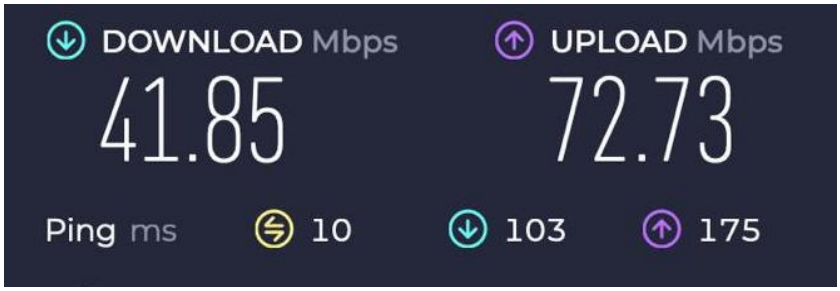


Рисунок 6.4 – Приклад вимірів до активації джерел інтерференції




```
% iperf3 -c iperf3.moji.fr
Connecting to host iperf3.moji.fr, port 5201
[  7] local 192.168.40.248 port 59915 connected to 45.147.210.189 port 5201
[ ID] Interval           Transfer     Bitrate
[  7]   0.00-1.01   sec  9.75 MBytes  81.4 Mbits/sec
[  7]   1.01-2.00   sec  8.25 MBytes  69.3 Mbits/sec
[  7]   2.00-3.00   sec  9.12 MBytes  76.8 Mbits/sec
[  7]   3.00-4.00   sec  8.88 MBytes  74.5 Mbits/sec
[  7]   4.00-5.00   sec  8.50 MBytes  71.1 Mbits/sec
[  7]   5.00-6.00   sec  6.62 MBytes  55.5 Mbits/sec
[  7]   6.00-7.01   sec  10.2 MBytes  86.0 Mbits/sec
[  7]   7.01-8.00   sec  8.88 MBytes  74.6 Mbits/sec
[  7]   8.00-9.01   sec  8.50 MBytes  71.2 Mbits/sec
[  7]   9.01-10.01  sec  6.00 MBytes  50.3 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  7]   0.00-10.01  sec  84.8 MBytes  71.1 Mbits/sec                  sender
[  7]   0.00-10.12  sec  84.1 MBytes  69.7 Mbits/sec                  receiver
```

```
% ping -s 1024 8.8.8.8 -c 25
PING 8.8.8.8 (8.8.8.8): 1024 data bytes
1032 bytes from 8.8.8.8: icmp_seq=0 ttl=115 time=87.162 ms
1032 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=42.214 ms
1032 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=36.334 ms
1032 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=143.209 ms
1032 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=45.488 ms
1032 bytes from 8.8.8.8: icmp_seq=5 ttl=115 time=43.161 ms
1032 bytes from 8.8.8.8: icmp_seq=6 ttl=115 time=153.351 ms
1032 bytes from 8.8.8.8: icmp_seq=7 ttl=115 time=35.640 ms
1032 bytes from 8.8.8.8: icmp_seq=8 ttl=115 time=35.753 ms
1032 bytes from 8.8.8.8: icmp_seq=9 ttl=115 time=46.697 ms
1032 bytes from 8.8.8.8: icmp_seq=10 ttl=115 time=48.931 ms
1032 bytes from 8.8.8.8: icmp_seq=11 ttl=115 time=44.415 ms
1032 bytes from 8.8.8.8: icmp_seq=12 ttl=115 time=43.618 ms
1032 bytes from 8.8.8.8: icmp_seq=13 ttl=115 time=43.952 ms
1032 bytes from 8.8.8.8: icmp_seq=14 ttl=115 time=34.689 ms
1032 bytes from 8.8.8.8: icmp_seq=15 ttl=115 time=51.127 ms
1032 bytes from 8.8.8.8: icmp_seq=16 ttl=115 time=44.195 ms
1032 bytes from 8.8.8.8: icmp_seq=17 ttl=115 time=37.189 ms
1032 bytes from 8.8.8.8: icmp_seq=18 ttl=115 time=48.181 ms
1032 bytes from 8.8.8.8: icmp_seq=19 ttl=115 time=43.895 ms
1032 bytes from 8.8.8.8: icmp_seq=20 ttl=115 time=44.524 ms
1032 bytes from 8.8.8.8: icmp_seq=21 ttl=115 time=43.700 ms
1032 bytes from 8.8.8.8: icmp_seq=22 ttl=115 time=37.761 ms
1032 bytes from 8.8.8.8: icmp_seq=23 ttl=115 time=41.469 ms
1032 bytes from 8.8.8.8: icmp_seq=24 ttl=115 time=44.671 ms

--- 8.8.8.8 ping statistics ---
25 packets transmitted, 25 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 34.689/52.853/153.351/29.790 ms
```

Рисунок 6.5 – Приклад вимірів після активації джерел інтерференції

КОНТРОЛЬНІ ЗАПИТАННЯ

Основні поняття та терміни

1. Що таке SSID, і яку роль він відіграє в мережі Wi-Fi?
2. Які основні частотні діапазони використовуються в мережах Wi-Fi?
3. Що таке точка доступу, і яка її роль у Wi-Fi мережі?

Продуктивність Wi-Fi

4. Як вибір каналу впливає на продуктивність мережі Wi-Fi?
5. Що таке інтерференція в контексті Wi-Fi, і як вона впливає на якість з'єднання?
6. Як фізичні перешкоди (стіни, меблі) впливають на рівень сигналу Wi-Fi?
7. Що таке потужність сигналу, і як вона впливає на зону покриття Wi-Fi мережі?

Безпека Wi-Fi

8. Які типи шифрування використовуються в Wi-Fi мережах, і який з них найбільш безпечний?

Стандарт 802.11

9. Що таке стандарт 802.11, і яку роль він відіграє у бездротових мережах?
10. Які основні відмінності між стандартами 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, і 802.11ax?
11. Які максимальні швидкості передачі даних забезпечують різні стандарти 802.11?
12. У яких частотних діапазонах працюють стандарти 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac і 802.11ax?
13. Як стандарти 802.11 впливають на зону покриття та пропускну здатність мережі?
14. Що таке MIMO, і як цей принцип використовується в стандартах 802.11n та 802.11ac?
15. Які нові функції і вдосконалення представлено у стандарті 802.11ax (Wi-Fi 6)?

Лабораторна робота №7

ТЕМА: СКАНУВАННЯ IP-МЕРЕЖ З ДОВІЛЬНОЮ КІЛЬКІСТЮ ОБ'ЄКТІВ ТА ВИЗНАЧЕННЯ ЇХ ВЛАСТИВОСТЕЙ

МЕТА: Отримати практичні навики роботи з утилітою Nmap з графічною оболонкою Zenmap.

ЗНАТИ: Основи мережної взаємодії.

ТЕОРЕТИЧНІ ВІДОМОСТІ

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором):

– https://nmap.org/download.html.

– https://nmap.org/book/man-examples.html.

– https://securitytrails.com/blog/nmap-commands.

– https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt.

– https://www.youtube.com/watch?v=-0jeplHyXmQ.

– https://nmap.org/book/zenmap-topology.html.

– https://www.youtube.com/watch?v=wt_xMols4Ww&ab_channel=CISOGlobal.

– https://www.youtube.com/watch?v=Xqj12-03vlg&ab_channel=RedBlueLabs.

ЗАВДАННЯ

Визначивши свій індивідуальний варіант завдання відповідно до списку наданого у курсі “Комп’ютерні мережі” у файлі індивідуальний варіант завдання студента (https://moodle.kntu.kr.ua/course/view.php?id=1035).

ЧАСТИНА 1 – ОСОБЛИВОСТІ ЗАСТОСУАВННЯ NMAP.

На основі визначеного індивідуального варіанту з дотриманням академічної доброчесності відповісти на наступні питання:

Варіант 1:

– У корпоративній мережі з IP-діапазоном 192.168.50.0/24 необхідно виявити всі пристрої, що мають відкритий порт 3389/tcp (Remote Desktop Protocol), але мережа захищена брандмауером, який блокує стандартні сканування. Які методи та параметри nmap ви використаєте для обходу брандмауера та виявлення потрібних хостів? Обґрунтуйте свій вибір і оцініть потенційні ризики.

– У останній бета-версії nmap була представлена нова опція --quantum-scan, яка використовує квантові алгоритми для оптимізації сканування мережі. Як ви можете застосувати цю опцію для підвищення ефективності сканування великої розподіленої мережі? Опишіть можливі переваги та ризики використання квантового сканування в контексті мережевої безпеки.

– Яка команда Nmap використовується для виконання прихованого сканування SYN?

Варіант 2:

– Потрібно визначити операційні системи хостів у мережі 10.1.1.0/24, але пряме сканування заборонено політиками безпеки. Яким чином можна використати пасивні можливості nmap або інші інструменти для збору цієї інформації без відправки скануючих пакетів? Опишіть процес та можливі обмеження.

– Під час аудиту мережі ви зіткнулися з пристроями, які відповідають на запити протоколом ZyberFlux на нестандартному порту 4567. Використовуючи nmap, як можна визначити версію цього протоколу та перевірити його на відомі вразливості? Які скрипти або методи ви будете застосовувати?.

– Яка команда Nmap використовується для повного TCP-з'єднання під час сканування?.

Варіант 3:

– Яка команда Nmap використовується для сканування UDP-портів?

– У мережі виявлено новий тип брандмауера, який використовує технологію HyperThread Cloaking для приховування відкритих портів. Як можна обійти цю технологію за допомогою nmap і які методи сканування для цього підходять? Оцініть ефективність цих методів і можливі наслідки.

– Ви помітили, що один з серверів у вашій мережі відповідає на запити дуже повільно. Потрібно визначити, чи є це наслідком високого навантаження або мережевих проблем. Як можна використати nmap для

діагностики цієї ситуації? Які параметри та методи ви застосуєте? Поясніть, як інтерпретувати отримані результати.

Варіант 4:

– Яка команда Nmap використовується для визначення версій сервісів на портах?

– Ви отримали завдання провести сканування з використанням опції --nano-ping, яка дозволяє відправляти наносекундні ICMP запити для визначення активності хостів з мінімальним впливом на мережу. Опишіть, як ви будете використовувати цю опцію та які переваги вона надає порівняно зі стандартними методами пінгу.

– Вашій команді потрібно провести аудит безпеки мережі, але ви хочете уникнути можливих порушень політик безпеки та випадкових збоїв в роботі систем. Як можна використати nmap для безпечного сканування, мінімізуючи ризики? Які параметри та підходи ви оберете? Обґрунтуйте свій вибір.

Варіант 5:

– Під час сканування мережі ви отримали нетипові результати: деякі порти відображаються як "open|filtered", а інші як "filtered". Що означають ці стани портів у nmap і як можна точніше визначити їх статус? Які додаткові методи сканування ви можете застосувати? Обґрунтуйте свій вибір.

– Опишіть принцип роботи Spectral Analysis Mode та його можливості. Розгляньте етичні аспекти використання технологій, що можуть порушувати приватність або безпеку обладнання.

– Яка команда Nmap використовується для визначення операційної системи хоста?

Варіант 6:

– Яка команда Nmap використовується для агресивного сканування із збором додаткової інформації?

– Ви хочете автоматизувати процес сканування мережі та отримувати результати у зручному для обробки форматі. Як можна використовувати nmap для виводу результатів у XML та подальшої їх обробки? Наведіть приклад команди та опишіть, як можна використати отримані дані в автоматизованих скриптах.

– Ви помітили, що деякі хости у вашій мережі використовують шифрування типу EnigmaShield для захисту своїх служб. Як за допомогою nmap можна виявити та проаналізувати такі служби? Які підходи та опції ви застосуєте?

Варіант 7:

– Яка команда Nmap використовується для сканування лише 80-го порту?

– Під час аудиту мережі ви виявили хости, які використовують застарілі протоколи та служби. Як можна за допомогою nmap виявити вразливості на цих хостах? Які скрипти та параметри ви будете використовувати? Опишіть процес і потенційні обмеження.

– Компанія впровадила новий протокол зв'язку ProtoX для внутрішніх сервісів. Він працює на порту 7890 і не сумісний зі стандартними протоколами. Як ви можете налаштувати nmap для сканування цього протоколу та які інструменти або скрипти можуть допомогти в його аналізі?

Варіант 8:

– Яка команда Nmap використовується для сканування всіх портів на хості?

– Під час тестування ви використовували опцію --stealth-mode в nmap, яка дозволяє сканувати мережу без генерування жодного мережевого трафіку. Поясніть, як це можливо і які методи використовуються для такого сканування. Оцініть практичність і достовірність результатів, отриманих цим способом.

– Ви бажаєте перевірити доступність певного порту (наприклад, 22/tcp) на великій кількості IP-адрес, зчитаних з файлу ip_list.txt. Як можна оптимізувати nmap для швидкого виконання цього завдання? Які параметри ви використаєте? Обґрунтуйте свій вибір.

Варіант 9:

– У вас є підозра, що в мережі діє зловмисник, який встановив прихований сервіс на нестандартному порту. Як можна за допомогою nmap виявити незвичні служби або порти, які зазвичай не використовуються? Які параметри та методи ви застосуєте? Опишіть свій підхід.

– Ви хочете використовувати функцію nmap під назвою Adaptive AI Scanning, яка автоматично налаштовує параметри сканування на основі попереднього аналізу мережі. Як ця функція може покращити ефективність сканування та які ризики пов'язані з використанням штучного інтелекту в цьому контексті?

– Яка команда Nmap використовується для швидкого сканування популярних портів?

Варіант 10:

– Яка команда Nmap використовується для перевірки активності хостів без сканування портів?

– У останній бета-версії nmap була представлена нова опція --quantum-scan, яка використовує квантові алгоритми для оптимізації сканування мережі. Як ви можете застосувати цю опцію для підвищення ефективності сканування великої розподіленої мережі? Опишіть можливі переваги та ризики використання квантового сканування в контексті мережевої безпеки.

– Під час сканування мережі ви хочете мінімізувати вплив на цільові хости і уникнути записів у журналах їх систем. Які методи сканування nmap ви можете використовувати для досягнення цього? Обґрунтуйте свій вибір та опишіть можливі етичні наслідки.

Варіант 11:

– У вашій мережі з'явився підозрілий хост з IP-адресою 172.16.10.25. Вам потрібно визначити, які служби на ньому працюють, але хост блокує стандартні методи сканування і відповідає повільно. Які методи та параметри nmap ви будете використовувати для успішного сканування цього хоста? Обґрунтуйте свій вибір та поясніть можливі ризики.

– Новий модуль nmap під назвою --deep-learning-probe дозволяє передбачати вразливості хостів на основі аналізу мережевих патернів. Як ви можете інтегрувати цей модуль у процес аудиту безпеки та які дані потрібні для його ефективної роботи? Обговоріть можливі етичні та технічні виклики.

– Яка команда Nmap використовується для визначення маршруту до цільового хоста?

Варіант 12:

– Яка команда Nmap використовується для прискорення сканування за допомогою таймінгу T4?

– Під час аудиту мережі ви зіткнулися з пристроями, які відповідають на запити протоколом ZyberFlux на нестандартному порту 4567. Використовуючи nmap, як можна визначити версію цього протоколу та перевірити його на відомі вразливості? Які скрипти або методи ви будете застосовувати?

– Ви хочете провести сканування мережі 10.0.0.0/16 для виявлення хостів з відкритими портами, але сканування великого діапазону IP-адрес може створити надмірне навантаження на мережу. Як можна ефективно сканувати цю мережу за допомогою nmap, мінімізуючи вплив на мережевий трафік? Які параметри ви будете використовувати?

Варіант 13:

– Яка команда Nmap використовується для повільного сканування з найменшим навантаженням на мережу?

– Під час аудиту ви бажаєте виявити хости, на яких працюють веб-сервери з вразливими версіями OpenSSL. Як за допомогою nmap визначити такі хости та перевірити їх на наявність конкретної вразливості, наприклад, Heartbleed (CVE-2014-0160)? Які скрипти ви будете використовувати?

– У мережі виявлено новий тип брандмауера, який використовує технологію HyperThread Cloaking для приховування відкритих портів. Як можна обійти цю технологію за допомогою nmap і які методи сканування для цього підходять? Оцініть ефективність цих методів і можливі наслідки.

Варіант 14:

– Яка команда Nmap використовується для проведення лише пінг-тесту?

– Ви отримали завдання провести сканування з використанням опції --nano-ping, яка дозволяє відправляти наносекундні ICMP запити для визначення активності хостів з мінімальним впливом на мережу. Опишіть, як ви будете використовувати цю опцію та які переваги вона надає порівняно зі стандартними методами пінгу.

– Ви помітили, що деякі хости у мережі відповідають некоректно на TCP SYN пакети. Як можна використати nmap для діагностики та розуміння причини такої поведінки? Які параметри та методи ви застосуєте?

Варіант 15:

– Яка команда Nmap використовується для сканування без попереднього пінгування хостів?

– Опишіть принцип роботи Spectral Analysis Mode та його можливості. Розгляньте етичні аспекти використання технологій, що можуть порушувати приватність або безпеку обладнання.

– У вашій організації планується впровадження IPv6, і вам потрібно перевірити, які хости вже підтримують цей протокол. Як за допомогою nmap можна сканувати мережу на наявність IPv6 хостів та які особливості потрібно враховувати?

Варіант 16:

– Потрібно перевірити, чи є в мережі хости, на яких працюють небезпечні або небажані служби, такі як Telnet або FTP з анонімним доступом. Як можна за допомогою nmap виявити такі служби та перевірити можливість анонімного входу?

– Ви помітили, що деякі хости у вашій мережі використовують шифрування типу EnigmaShield для захисту своїх служб. Як за допомогою nmap можна виявити та проаналізувати такі служби? Які підходи та опції ви застосуєте?

– Яка команда Nmap використовується для сканування мережі за допомогою IPv6?

Варіант 17:

– Компанія впровадила новий протокол зв'язку ProtoX для внутрішніх сервісів. Він працює на порту 7890 і не сумісний зі стандартними протоколами. Як ви можете налаштувати nmap для сканування цього протоколу та які інструменти або скрипти можуть допомогти в його аналізі?

– У мережі є декілька пристроїв, які працюють під управлінням операційної системи Windows, але мають вимкнений ICMP (ping) та деякі TCP порти. Як можна за допомогою nmap виявити ці хости та перевірити, які порти на них відкриті?

– Яка команда Nmap використовується для отримання причин відкриття чи закриття порту?

Варіант 18:

– Вам потрібно провести сканування мережі, але згенерувати мінімальну кількість записів у журналах цільових систем. Як можна налаштувати nmap для цього, і які методи сканування підходять найкраще? Обґрунтуйте свій вибір.

– Під час тестування ви використовували опцію --stealth-mode в nmap, яка дозволяє сканувати мережу без генерування жодного мережевого трафіку. Поясніть, як це можливо і які методи використовуються для такого сканування. Оцініть практичність і достовірність результатів, отриманих цим способом.

– Яка команда Nmap використовується для фільтрації лише відкритих портів у виводі?

Варіант 19:

– Яка команда Nmap використовується для отримання заголовків HTTP-сайтів за допомогою скрипта?

– Ви хочете використовувати функцію nmap під назвою Adaptive AI Scanning, яка автоматично налаштовує параметри сканування на основі попереднього аналізу мережі. Як ця функція може покращити ефективність сканування та які ризики пов'язані з використанням штучного інтелекту в цьому контексті?

– Потрібно провести сканування мережі та автоматично виконати специфічні дії на основі результатів сканування. Наприклад, якщо на хості відкритий порт 80, запустити перевірку вразливостей веб-серверів. Як можна інтегрувати nmap з іншими інструментами або скриптами для автоматизації такого процесу?

Варіант 20:

– Яка команда Nmap використовується для перевірки уразливостей в мережі?

– У останній бета-версії nmap була представлена нова опція --quantum-scan, яка використовує квантові алгоритми для оптимізації сканування мережі. Як ви можете застосувати цю опцію для підвищення ефективності сканування великої розподіленої мережі? Опишіть можливі переваги та ризики використання квантового сканування в контексті мережевої безпеки.

– Під час сканування ви хочете використовувати скрипти nmap для виявлення відомих вразливостей у службах, що працюють на хостах мережі. Як можна визначити, які скрипти доступні для певних служб, та як їх правильно застосувати? Наведіть приклади.

Варіант 21:

– Яка команда Nmap використовується для аналізу SSL-сертифікатів на хості?

– Новий модуль nmap під назвою --deep-learning-probe дозволяє передбачати вразливості хостів на основі аналізу мережевих патернів. Як ви можете інтегрувати цей модуль у процес аудиту безпеки та які дані потрібні для його ефективної роботи? Обговоріть можливі етичні та технічні виклики.

– Ви бажаєте виконати сканування мережі, але ваша IP-адреса потрапила до чорного списку деяких хостів. Як можна використовувати техніку підміни IP-адреси (IP spoofing) у nmap для обходу цього обмеження? Які обмеження та ризики пов'язані з цим методом?

Варіант 22:

– Яка команда Nmap використовується для виконання Xmas-сканування?

– Під час аудиту мережі ви зіткнулися з пристроями, які відповідають на запити протоколом ZyberFlux на нестандартному порту 4567. Використовуючи nmap, як можна визначити версію цього протоколу та перевірити його на відомі вразливості? Які скрипти або методи ви будете застосовувати?

– Під час сканування мережі ви хочете використовувати власні TCP або UDP пакети з налаштованими прапорами та даними. Як можна використовувати nmap для створення та відправки таких спеціальних пакетів? Які можливості для цього надає nmap?

Варіант 23:

– Яка команда Nmap використовується для проведення Null-сканування?

– У мережі виявлено новий тип брандмауера, який використовує технологію HyperThread Cloaking для приховування відкритих портів. Як можна обійти цю технологію за допомогою nmap і які методи сканування для цього підходять? Оцініть ефективність цих методів і можливі наслідки.

– Вам потрібно виконати сканування мережі через проміжний проксі-сервер або тунель SSH. Як можна налаштувати nmap для роботи в такому середовищі? Які обмеження існують?

Варіант 24:

– Потрібно провести сканування мережі, але приховати факт сканування від систем виявлення вторгнень (IDS). Які методи nmap можна використовувати для уникнення виявлення, і які параметри слід налаштувати? Обговоріть ефективність та ризики.

– Ви отримали завдання провести сканування з використанням опції --nano-ping, яка дозволяє відправляти наносекундні ICMP запити для визначення активності хостів з мінімальним впливом на мережу. Опишіть, як

ви будете використовувати цю опцію та які переваги вона надає порівняно зі стандартними методами пінгу.

– Яка команда Nmap використовується для виконання FIN-сканування?

Варіант 25:

– Яка команда Nmap використовується для проведення Idle-сканування?

– Опишіть принцип роботи Spectral Analysis Mode та його можливості. Розгляньте етичні аспекти використання технологій, що можуть порушувати приватність або безпеку обладнання.

– Ви бажаєте використовувати nmap для моніторингу змін у мережі з часом. Як можна автоматизувати сканування та порівняння результатів для виявлення нових або зниклих хостів та служб? Які інструменти та методи можна застосувати?

Варіант 26:

– Під час сканування ви хочете зібрати якомога більше інформації про банери служб та можливі приховані служби. Як можна налаштувати nmap для глибшого дослідження та які опції використовувати?

– Ви помітили, що деякі хости у вашій мережі використовують шифрування типу EnigmaShield для захисту своїх служб. Як за допомогою nmap можна виявити та проаналізувати такі служби? Які підходи та опції ви застосуєте?

– Яка команда Nmap використовується для додавання даних до пакетів при скануванні?

Варіант 27:

– Ви хочете перевірити стійкість мережі до масових сканувань та можливих атак. Як можна симулювати масове сканування за допомогою nmap та які параметри слід використовувати? Які заходи безпеки слід врахувати при цьому?

– Компанія впровадила новий протокол зв'язку ProtoX для внутрішніх сервісів. Він працює на порту 7890 і не сумісний зі стандартними протоколами. Як ви можете налаштувати nmap для сканування цього протоколу та які інструменти або скрипти можуть допомогти в його аналізі?

– Яка команда Nmap використовується для обмеження кількості повторів при скануванні?

Варіант 28:

– Яка команда Nmap використовується для встановлення мінімальної швидкості сканування?

– Під час тестування ви використовували опцію --stealth-mode в nmap, яка дозволяє сканувати мережу без генерування жодного мережевого трафіку. Поясніть, як це можливо і які методи використовуються для такого

сканування. Оцініть практичність і достовірність результатів, отриманих цим способом.

– Потрібно перевірити, чи є у мережі хости, що використовують слабкі або дефолтні паролі для служб SSH. Як можна за допомогою nmap та його скриптів виявити такі хости? Які етичні аспекти слід врахувати?

Варіант 29:

– Яка команда Nmap використовується для обмеження максимальної швидкості сканування?

– Ви хочете використовувати функцію nmap під назвою Adaptive AI Scanning, яка автоматично налаштовує параметри сканування на основі попереднього аналізу мережі. Як ця функція може покращити ефективність сканування та які ризики пов'язані з використанням штучного інтелекту в цьому контексті?

– Ви бажаєте дослідити використання протоколу IPv6 у вашій мережі та виявити можливі вразливості. Які інструменти та методи nmap можна застосувати для сканування IPv6, та які особливості слід врахувати?

Варіант 30:

– Під час сканування ви хочете виявити хости, що працюють у віртуальних середовищах або є емуляцією. Як можна за допомогою nmap визначити такі хости та які ознаки про це свідчать?

– У останній бета-версії nmap була представлена нова опція --quantum-scan, яка використовує квантові алгоритми для оптимізації сканування мережі. Як ви можете застосувати цю опцію для підвищення ефективності сканування великої розподіленої мережі? Опишіть можливі переваги та ризики використання квантового сканування в контексті мережевої безпеки.

– Яка команда Nmap використовується для отримання детального виводу для діагностики?

Варіант 31:

– Яка команда Nmap використовується для сканування з некоректною контрольною сумою?

– Ви хочете перевірити мережу на наявність відкритих проксі-серверів, які можуть бути використані зловмисниками. Як можна за допомогою nmap виявити такі хости та перевірити їхню вразливість?

– Новий модуль nmap під назвою --deep-learning-probe дозволяє передбачати вразливості хостів на основі аналізу мережевих патернів. Як ви можете інтегрувати цей модуль у процес аудиту безпеки та які дані потрібні для його ефективної роботи? Обговоріть можливі етичні та технічні виклики.

Варіант 32:

– Потрібно перевірити, чи є в мережі хости, які працюють з небезпечними версіями протоколу SSL/TLS. Як можна за допомогою nmap визначити версії протоколів SSL/TLS та виявити вразливості?

– Під час аудиту мережі ви зіткнулися з пристроями, які відповідають на запити протоколом ZyberFlux на нестандартному порту 4567. Використовуючи nmap, як можна визначити версію цього протоколу та перевірити його на відомі вразливості? Які скрипти або методи ви будете застосовувати?

– Яка команда Nmap використовується для фрагментації пакетів при скануванні?

Варіант 33:

– Яка команда Nmap використовується для обходу обмежень швидкості відповіді RST?

– Ви хочете визначити, чи є у мережі хости, що відповідають на SNMP запити з дефолтною або слабкою спільнотою (community string). Як можна за допомогою nmap виявити такі хости та які скрипти використовувати?

– У мережі виявлено новий тип брандмауера, який використовує технологію HyperThread Cloaking для приховування відкритих портів. Як можна обійти цю технологію за допомогою nmap і які методи сканування для цього підходять? Оцініть ефективність цих методів і можливі наслідки.

Варіант 34:

– Яка команда Nmap використовується для випадкового порядку сканування хостів?

– Під час аудиту мережі ви хочете перевірити, чи є уразливі до атак типу "man-in-the-middle" хости з відкритими RDP службами. Як можна за допомогою nmap перевірити безпеку RDP служб?

– Ви отримали завдання провести сканування з використанням опції --nano-ping, яка дозволяє відправляти наносекундні ICMP запити для визначення активності хостів з мінімальним впливом на мережу. Опишіть, як ви будете використовувати цю опцію та які переваги вона надає порівняно зі стандартними методами пінгу.

Варіант 35:

– Яка команда Nmap використовується для збереження результатів сканування у звичайному текстовому форматі?

– Опишіть принцип роботи Spectral Analysis Mode та його можливості. Розгляньте етичні аспекти використання технологій, що можуть порушувати приватність або безпеку обладнання.

– Ви бажаєте дослідити можливість DNS зонної передачі (zone transfer) на DNS-серверах у мережі. Як можна за допомогою nmap перевірити, чи дозволяє DNS-сервер зонну передачу, та які скрипти для цього використовуються?

Варіант 36:

– Яка команда Nmap використовується для збереження результатів у форматі XML?

– Ви помітили, що деякі хости у вашій мережі використовують шифрування типу EnigmaShield для захисту своїх служб. Як за допомогою nmap можна виявити та проаналізувати такі служби? Які підходи та опції ви застосуєте?

– Під час сканування ви хочете виявити хости, які відповідають на HTTP-запити, але не на стандартному порту 80. Як можна за допомогою nmap знайти такі хости у мережі?

Варіант 37:

– Яка команда Nmap використовується для збереження результатів у фільтрованому форматі (gnmap)?

– Ви хочете перевірити мережу на наявність хостів з відкритими базами даних, такими як MongoDB або Elasticsearch, які можуть бути вразливі до несанкціонованого доступу. Як можна за допомогою nmap виявити такі хости та перевірити їхню безпеку?

– Компанія впровадила новий протокол зв'язку ProtoX для внутрішніх сервісів. Він працює на порту 7890 і не сумісний зі стандартними протоколами. Як ви можете налаштувати nmap для сканування цього протоколу та які інструменти або скрипти можуть допомогти в його аналізі?

Варіант 38:

– Потрібно провести сканування мережі та автоматично згенерувати звіт у форматі HTML для подальшого представлення керівництву. Як можна налаштувати nmap для виводу результатів у форматі, придатному для конвертації в HTML, та які інструменти можна використати для цієї конвертації?

– Під час тестування ви використовували опцію --stealth-mode в nmap, яка дозволяє сканувати мережу без генерування жодного мережевого трафіку. Поясніть, як це можливо і які методи використовуються для такого сканування. Оцініть практичність і достовірність результатів, отриманих цим способом.

– Яка команда Nmap використовується для сканування хостів із файлу?

Варіант 39:

– Ви бажаєте перевірити, чи є в мережі хости, що використовують небезпечні версії програмного забезпечення, наприклад, старі версії OpenSSH. Як можна за допомогою nmap виявити такі хости та автоматично визначити, чи вони вразливі?

– Ви хочете використовувати функцію nmap під назвою Adaptive AI Scanning, яка автоматично налаштовує параметри сканування на основі

попереднього аналізу мережі. Як ця функція може покращити ефективність сканування та які ризики пов'язані з використанням штучного інтелекту в цьому контексті?

– Яка команда Nmap використовується для випадкового вибору хостів для сканування?

Варіант 40:

– Яка команда Nmap використовується для обмеження кількості повторів при скануванні?

– У останній бета-версії nmap була представлена нова опція --quantum-scan, яка використовує квантові алгоритми для оптимізації сканування мережі. Як ви можете застосувати цю опцію для підвищення ефективності сканування великої розподіленої мережі? Опишіть можливі переваги та ризики використання квантового сканування в контексті мережевої безпеки.

– Під час сканування ви хочете використовувати nmap для виявлення хостів з активними службами VPN, які можуть бути потенційними точками витоку інформації. Як можна за допомогою nmap виявити такі хости та які порти та скрипти слід використовувати?

ЧАСТИНА 2 – ОСНОВИ ПРАКТИЧНОГО ВИКОРИСТАННЯ NMAP

Використовуючи безкоштовне програмне забезпечення для дослідження та аудиту безпеки мереж nmap (Network Mapper) провести сканування тестового серверу у глобальній мережі Інтернет

scanme.nmap.org

Знайти відповідь на наступні запитання:

1. Яка IP адреса сервера?

2. Яка операційна система встановлена на сервері?

3. Вкажіть стан портів (open, filtered) та які саме порти задіянні на сервері?

4. Яка версія OpenSSH використовується?

5. Визначте повний трасувальний шлях (traceroute) від локального ПК до сервера з проміжними вузлами що проходять через Україну у вигляді топологічної ланки (приклад на рисунку 7.1).

6. Яка геолокація сервера?

7. Якій використовується провайдер (платформа) хмарних обчислень де

базується сервер?

При скануванні серверу дотримуватись доброчесного поводження з сервером, не DDOS атаки та ін. більш детально можна подивіться по посиланню http://scanme.nmap.org/.

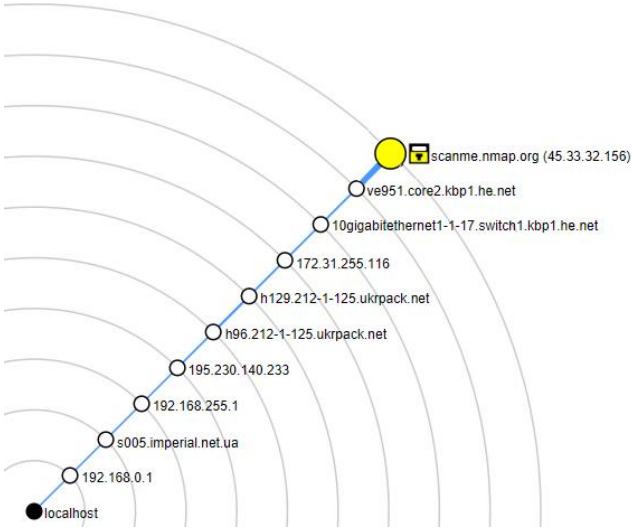


Рисунок 7.1 – Шаблон локальної мережі кафедри КБПЗ

ЧАСТИНА 3 – ВИКОНУЄТЬСЯ НА ОБЛАДНАННІ КАФЕДРИ.

3.1. Визначити адресацію локальної мережі кафедри КБПЗ. Провести сканування локальної мережі використовуючи безкоштовне програмне забезпечення для дослідження та аудиту безпеки мереж nmap (Network Mapper).

Заповнити наданий шаблон знайденими підмережами, на рисунку 7.1 представлено приклад, де ??? це IP:XX.XX.XX.XX/XX, у доданих файлах л/р є варіант у форматі draw.io для зручності.

Створити за допомогою Zenmap топологію локальної мережі кафедри приклад формування представлено на рисунку 7.2.

3.2. На основі визначеного індивідуального варіанту IP адреси (однаковий до всієї л.р.) визначити наступне:

1. Визначити відкриті TCP/IP порти.

2. Встановити які сервіси працюють на цих портах.

3. Зайти в одному із знайдених портів термінал та визначити ІНДИВІДУАЛЬНИЙ КОД ВАРІАНТУ. Якщо знайдені сервіси запитують пароль, по замовчанню використовується admin/admin.

Варіанти IP у відповідності до індивідуального варіанту:

Варіант 1 IP: 192.168.200.201;

Варіант 2 IP: 192.168.200.202;

Варіант 3 IP: 192.168.200.203;

Варіант 4 IP: 192.168.200.204;

Варіант 5 IP: 192.168.200.205;

Варіант 6 IP: 192.168.200.206;

Варіант 7 IP: 192.168.200.207;

Варіант 8 IP: 192.168.200.208;

Варіант 9 IP: 192.168.200.209;

Варіант 10 IP: 192.168.200.210;

Варіант 11 IP: 192.168.200.211;

Варіант 12 IP: 192.168.200.212;

Варіант 13 IP: 192.168.200.213;

Варіант 14 IP: 192.168.200.214;

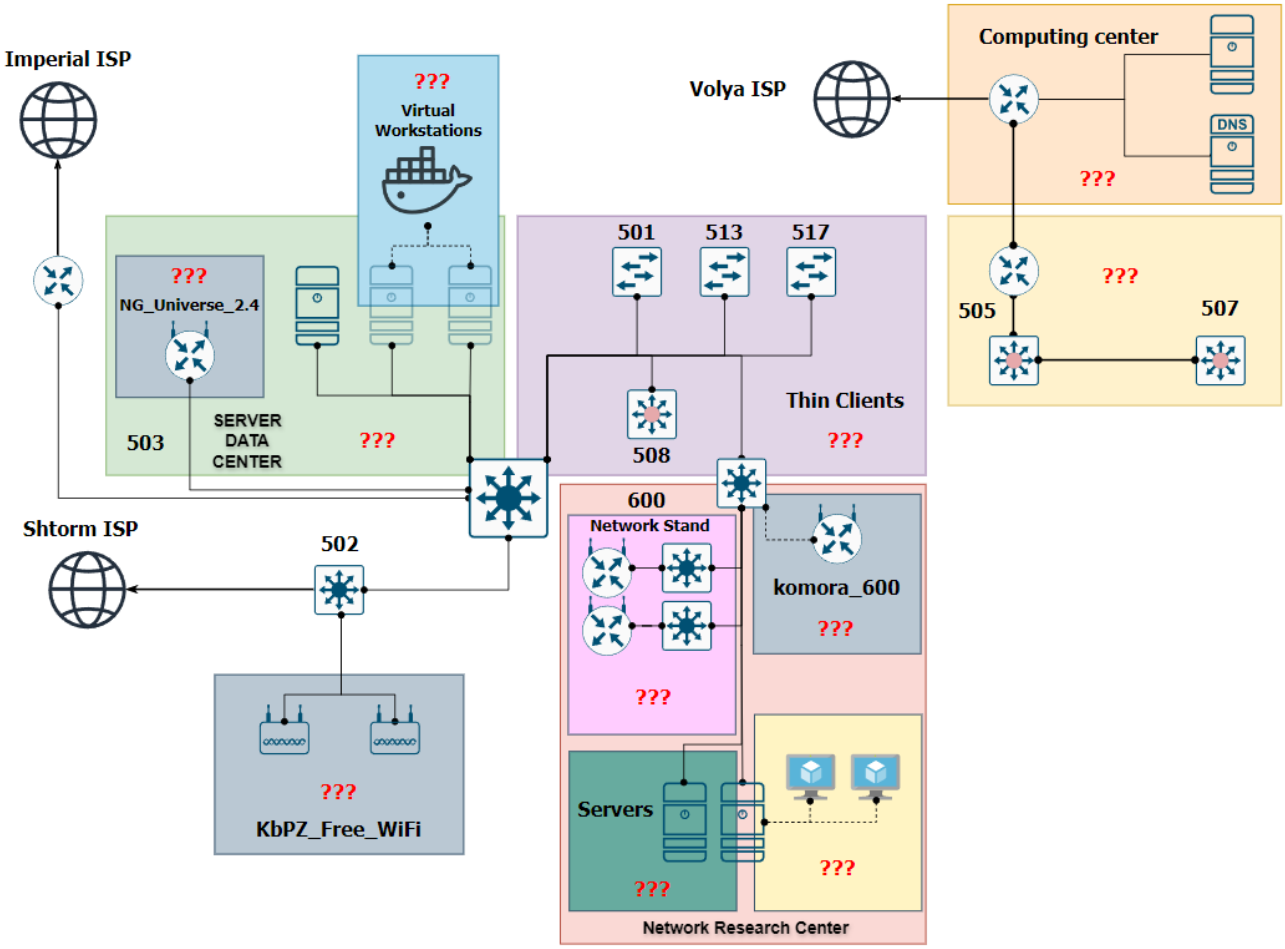


Рисунок 7.2 – Шаблон локальної мережі кафедри КБПЗ

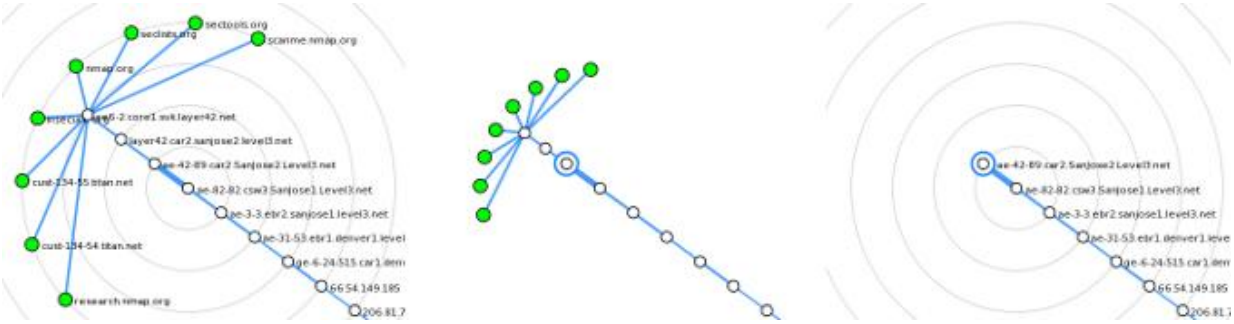


Рисунок 7.3 – Приклад частини локальної топології зірка

Варіант 15 IP: 192.168.200.215;

Варіант 16 IP: 192.168.200.216;

Варіант 17 IP: 192.168.200.217;

Варіант 18 IP: 192.168.200.218;

Варіант 19 IP: 192.168.200.219;

Варіант 20 IP: 192.168.200.220;

Варіант 21 IP: 192.168.200.221;

Варіант 22 IP: 192.168.200.222;

Варіант 23 IP: 192.168.200.223;

Варіант 24 IP: 192.168.200.224;

Варіант 25 IP: 192.168.200.225;

Варіант 26 IP: 192.168.200.226;

Варіант 27 IP: 192.168.200.227;

Варіант 28 IP: 192.168.200.228;

Варіант 29 IP: 192.168.200.229;

Варіант 30 IP: 192.168.200.230;

Варіант 31 IP: 192.168.200.231;

Варіант 32 IP: 192.168.200.232;

Варіант 33 IP: 192.168.200.233;

Варіант 34 IP: 192.168.200.234;

Варіант 35 IP: 192.168.200.235;

Варіант 36 IP: 192.168.200.236;

Варіант 37 IP: 192.168.200.237;

Варіант 38 IP: 192.168.200.238;

Варіант 39 IP: 192.168.200.239;

Варіант 40 IP: 192.168.200.240.

КОНТРОЛЬНІ ЗАПИТАННЯ

ЗАГАЛЬНІ ЗАПИТАННЯ

1. Навіщо потрібні порти TCP/IP?
2. Для чого необхідні мережні сканери портів?
3. За що відповідає організація IANA(www.iana.org)?

4. Які номери портів називаються загальновідомими?
5. Чим недовговічні номери портів відрізняються від загальновідомих?
6. Який номер порту TCP/IP використовує Telnet?
7. Який номер порту TCP/IP використовує FTP?
8. Який номер порту TCP/IP використовує SSH?
9. Який номер порту TCP/IP використовує SMTP?
10. Який номер порту TCP/IP використовує Pop3?
11. Який номер порту TCP/IP використовує DNS?
12. Який номер порту TCP/IP використовує HTTP?

NMAP (THE NETWORK MAPPER)

13. Що таке NMAP і які його основні функції?
14. Які основні типи сканування портів підтримує NMAP?
15. Як провести базове сканування всіх відкритих портів на хості за допомогою NMAP?
16. Які ключі командного рядка NMAP використовуються для визначення операційної системи цільової машини?
17. Як можна використовувати NMAP для виявлення версій сервісів, що працюють на відкритих портах?
18. Які ключі командного рядка NMAP використовуються для скритого (прихованого) сканування?

ZENMAP (NMAP SECURITY SCANNER GUI)

19. Що таке Zenmap і яка його роль в роботі з NMAP?
20. Які основні переваги використання графічного інтерфейсу Zenmap у порівнянні з командним рядком NMAP?

Лабораторна робота №8

ТЕМА: БАЗОВЕ ПЕРЕХОПЛЕННЯ І АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ В ЛОКАЛЬНІЙ МЕРЕЖІ

МЕТА Сформувати практичні навички виявлення активних вузлів локальної мережі, виконання мережевого сканування та аналізу пакетного трафіку, згенерованого у контрольованих умовах, із використанням інструментів моніторингу та аналізу мережі, виявлення відкритих портів та автентифікації через Telnet

ЗНАТИ: Основи взаємодії у локальних мережах

ТЕОРЕТИЧНІ ВІДОМОСТІ

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором):

– https://www.sciencedirect.com/science/article/pii/S111001682501110X A novel approach for real-time anomaly detection in real-time network traffic (Wireshark live data).

– https://www.sciencedirect.com/science/article/pii/S2405959525000050 Deep learning-driven methods for network-based intrusion detection systems: A systematic review.

– https://www.mdpi.com/2624-800X/4/4/37 Detection of Hacker Intention Using Deep Packet Inspection.

– https://www.sciencedirect.com/science/article/pii/S2405844024119937 Encrypted traffic classification based on federated learning (FedETC).

– https://www.mdpi.com/1424-8220/24/11/3509 Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning.

– https://publications.eai.eu/index.php/inis/article/view/7616 A novel approach for graph-based real-time anomaly detection from dynamic network data listened by Wireshark.

– https://www.mdpi.com/2076-3417/14/6/2409 A Novel Network Protocol Syntax Extracting Method for Network Protocol Fuzzing (using Wireshark dissector files).

– https://www.mdpi.com/2624-800X/5/4/94 Anomaly Detection Against Fake Base Station Threats (packets captured with Wireshark).

Рекомендовані інструменти

Wireshark – для виявлення IP-адреси пристрою та аналізу UDP-повідомлень.

Nmap – для сканування локальної підмережі, виявлення відкритих портів та

аналізу пристрою.

Telnet-клієнт – для встановлення з'єднання з відкритими портами та подальшої взаємодії з пристроєм.

ЗАВДАННЯ

ЧАСТИНА 1 – ЗАХОПЛЕННЯ ТРАФІКУ ЛОКАЛЬНОЇ МЕРЕЖІ

1.1 Підготовка

1. Спитати особливості підключення у викладача який проводе лабораторну роботу та під'єднати робочу станцію до виділеного сегмента локальної мережі лабораторії.

2. Зафіксувати власні параметри мережевого інтерфейсу (IP-адреса, маска, шлюз, DNS, MAC-адреса, тощо.).

3. Вказати індівідуальний варіант та дати запит викладачу який проводе лабораторну роботу на генерацію пакетів трафіку.

1.2 Мережеве сканування

4. Увімкнути захоплення трафіку на відповідному мережевому

інтерфейсі в Wireshark (або еквіваленті).

5. Чекати вказівки викладача на завершення захоплення трафіку та формування файлу результату (рекомендується формат PCAPNG).

1.3 Аналіз контрольовано згенерованого трафіку

6. Під час виконання роботи викладач у контрольованому режимі генерує та передає у локальну мережу набір різнотипних пакетів (кадрів) потрібно детально проаналізувати та ідентифікувати особливості сформованого трафіку (визначити ключові параметри для кожного типу пакета, протоколи, заголовки і.т.д.).

1.4 Інтерпретація та узагальнення результатів

7. Сформувати висновок у вигляді звіту лабораторної роботи, пояснити призначення кожної групи виявлених пакетів у контексті моделювання мережевої активності (наприклад: діагностика доступності, обмін службовою інформацією, ініціація з'єднань, запити імен/адрес тощо). Виявити потенційні індикатори мережевих подій: широкомовні/мультикаст-пакети, повторювані запити, аномальні значення полів заголовків, незвичні порти, нетипові частоти.

ОФОРМЛЕННЯ ЗВІТУ ПУНКТ 1

У звіт лабораторної роботи помістити:

– Завдання л/роботи.

– Покрокові матеріали що повністю підтверджують виконання л/роботи (текст, таблиці, принтскріни, та інші матеріали для підтвердження виконання л/роботи).

– Короткі змістовні відповіді на л/роботи.

Лабораторну роботу оформляти по загальноприйнятій формі (ДСТУ) та аналогічно до інших предметів кафедри КБПЗ ЦНТУ.

ЧАСТИНА 2 – ЗАХОПЛЕННЯ ТРАФІКУ ЛОКАЛЬНОЇ МЕРЕЖІ

2.1 Опис сценарію роботи з навчально-дослідницьким комплексом для відпрацювання навичок діагностики мережевої інфраструктури в умовах, наближених до реальної експлуатації «Mr. Rabbit Challenge»

ВИЯВЛЕННЯ ПРИСТРОЮ В БЕЗДРОТОВІЙ МЕРЕЖІ (WI-FI):

1. Пристрій (Mr. Rabbit) на базі мікроконтролера ESP32 періодично підключається до однієї з п’яти доступних Wi-Fi мереж. Конкретна мережа невідома, тому студент має самостійно виявити IP-адресу пристрою.

2. Аналіз UDP-трафіку: Пристрій кожні декілька секунд надсилає широкомовні UDP-пакети, які містять підказки для подальших дій. Завдання студента – проаналізувати ці пакети за допомогою Wireshark, визначити IP-адресу пристрою та зміст повідомлень.

3. Пошук Telnet-портів: На пристрої відкрито три порти («гостьові порти») в діапазоні 20-5000, які відповідають за первинну перевірку («тест на кролика»). Один із них дозволить пройти авторизацію та отримати доступ до додаткової інформації.

4. Виявлення прихованого порту: Після успішної перевірки на гостьовому порту, студент отримає дані про прихований Telnet-порт у діапазоні 5000-10000. Саме цей порт веде до основного інтерфейсу взаємодії з Mr. Rabbit.

5. Взаємодія з прихованим портом: На прихованому порту користувач має пройти автентифікацію, після чого ввести своє повне ім’я англійською мовою. У відповідь пристрій повертає індивідуальний псевдонім у форматі RABBITXXXXX.

6. Основна проблема це обмеження за часом – не рекомендується прямий перебор портів чи інтенсивне сканування:

– Telnet-сесія на гостьових портах – до 30 секунд.

– Telnet-сесія на прихованому порту – до 120 секунд.

– Кожні 10 хвилин пристрій змінює свою IP-адресу, порт та мережу, до якої його підключено, що вимагає повторного пошуку при невдалому проходженні.

2.2 АЛГОРИТМ ВИКОНАННЯ

1. Провести сканування підмережі засобами Nmap для виявлення IP з трьома відкритими портами в діапазоні 20-5000.

2. Підключитися до портів знайденої IP-адреси через Telnet, знайти порт, на якому Mr. Rabbit очікує свого друга.

3. За допомогою Wireshark, проаналізувавши UDP-трафік з адреси Mr. Rabbita, отримати IP з якого Mr. Rabbit очікує друга. Поміняти свій IP на знайдений.

4. Підключитися через Telnet до порту, на якому Mr. Rabbit очікує друга, пройти автентифікацію (rabbit/carrot). Отримати інформацію про прихований порт, логін та пароль.

5. Підключитися до прихованого порту, автентифікуватися. Ввести власне повне ім’я англійською. Отримати секретне кодове ім’я у форматі RABBITXXXXX.

ОФОРМЛЕННЯ ЗВІТУ ПУНКТ 2, ДОДАТИ НАСТУПНІ ДАНІ:

– Прізвище, ім’я, по батькові;

– Дата виконання завдання;

– Скріншоти з Wireshark (UDP-трафік, IP-адреса пристрою);

– Скріншоти з Nmap (результати сканування);

– Отримані логін та пароль до прихованого порту;

– Скріншоти сесій Telnet (гостьові та прихована нори);

– Отримане секретне ім’я у форматі RABBITXXXXX.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Яка різниця між пасивним аналізом трафіку та активним скануванням локальної мережі, і які ризики/обмеження має кожен підхід?

2. Які мережеві параметри робочої станції необхідно зафіксувати перед початком захоплення трафіку (IP, маска, шлюз, DNS, MAC) та чому це важливо для інтерпретації PCAP?

3. Що таке підмережа та CIDR, і як визначити діапазон адрес для коректного сканування в межах локального сегмента?

4. Які типові методи виявлення активних вузлів використовуються під час сканування (ARP/ICMP/TCP), і як вони відображаються у трафіку Wireshark?

5. Які мережеві протоколи найчастіше спостерігаються під час сканування локальної мережі (ARP, ICMP, TCP, UDP) та яку роль вони виконують?

6. Які ознаки у захопленому трафіку дозволяють відрізнити трафік сканування від фонового (часові мітки, повторюваність, адресація, порти, характерні прапорці TCP)?

7. Які ключові поля заголовків Ethernet, IPv4/IPv6 та TCP/UDP доцільно аналізувати для ідентифікації типу трафіку та його призначення?

8. Що означають прапорці TCP (SYN, ACK, FIN, RST, PSH, URG), і які їх типові комбінації характерні для SYN-scan та встановлення з’єднання?

9. Як у Wireshark застосовуються capture filters і display filters, у чому їх відмінність та коли доцільно використовувати кожен із них?

Система оцінювання та вимоги

Контроль знань і умінь (поточний і підсумковий) з дисципліни «**Комп'ютерні мережі**» здійснюється згідно з кредитною трансферно-накопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи, виконання лабораторних завдань).

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою
		для екзамену
90-100	A	Відмінно
82-89	B	Добре
74-81	C	
64-73	D	Задовільно
60-63	E	
35-59	FX	незадовільно з можливістю повторного складання
1-34	F	незадовільно з обов'язковим повторним вивченням дисципліни

Критерії оцінювання знань і вмінь здобувачів визначені Положенням про організацію освітнього процесу в ЦНТУ (*стор. 32-33*).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

Базова

1. Kovalenko O., Khudov H., Mynko P., Ikhsanov S., Diakonov O., Solomonenko Y., Drob Y., Kharun O., Cherkashyn S., Serdiuk O. «Development A Method For Determining The Coordinates Of Air Objects By Radars With The Additional Use Of Multilateration Technology» Eastern-European Journal of Enterprise Technologies Volume 5, 2021, Pages 6-16.
Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85119667497&origin=resultslist (Scopus).

2. Serhii Pohasii, Serhii Yevseiev, Oleksandr Zhuchenko, Oleksandr Milov, Volodymyr Lysechko, Oleksandr Kovalenko, Maryna Kostiak, Andrii Volkov, Aleksandr Lezik, Vitalii Susukailo «Development of crypto-code constructs based on LDPC codes» Eastern-European Journal of Enterprise Technologies 2/9 (116), 2022, Pages 44-59.
Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85130069202&origin=resultslist (Scopus).

3. Смірнова Т.В., Моторін Ю.Ю., Буравченко К.О., Бочуля Т.В., Коваленко О.В. «Вибір оптимальної технології побудови хмарної інформаційно-комунікаційної системи автоматизації виробничих процесів» Вимірювальна та обчислювальна техніка в технологічних процесах, № 1 (2022). С. 15-26. 2022. Режим доступу: http://vottp.khmnu.edu.ua/index.php/vottp/article/view/30/36 (Фахове видання. Категорія «Б»)

4. Khudov H., Baranik O., Kovalenko O.,Yakovenko Y., Chahan Y. «The Information Technology for Determining Vehicle Route Based on Ant Colony Algorithms» International Journal of Emerging Technology and Advanced Engineering, 2022, 12(12), Pages 117–128. Режим доступу:

https://www.scopus.com/record/display.uri?eid=2-s2.0-85130069202&origin=resultslist (Scopus).

5. Hennadii Khudov, Volodymyr Bashynskyi, Oleksandr Kovalenko, Kristina Tahyan, Oleksii Fakadii « The methods for improving the quality of detection of inconspicuous aerial objects through the use of external radiation sources» International Journal of Emerging Technology and Advanced Engineering, 2023, Volume 13, Issue 3, Pages 91-100. Режим доступу: https://doi.org/10.46338/ijetae0323_09 (Закордонне фахове видання).

6. Hennadii Khudov, Oleksandr Kostianets, Oleksandr Kovalenko, Oleh Maslenko, Yuriy Solomonenko «Using softwaredefined radio receivers for determining the coordinates of low-visible aerial objects» Eastern-European Journal of Enterprise Technologies Vol. 5 No. 9 (124), 2023, Pages 61-73. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85172343893&origin=resultslist (Scopus).

7. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». Центральноукраїнський науковий вісник. Технічні науки. 2025. Вип. 11(42), ч. II. С.52-62. Режим доступу: https://mapiea.kntu.kr.ua/pdf/11(42)_II/11(42)_II_2025.pdf (Фахове видання. Категорія «Б»)

8. Коваленко О.В. Моделі та методи розробки програмного забезпечення комп'ютерних систем для підвищення безпеки даних: монография / О.В. Коваленко // К.: Вид. «КОД» – 2019. – 350 с.

Читальний зал № 1 (ЦНТУ)

9. Глухов В. С., Костик А. Т. Дослідження і проектування комп'ютерних систем та мереж : навч. посіб. Львів : Магнолія 2006, 2025. 253 с. ISBN 978-

617-574-265-5. Режим доступу: https://opac.kntu.kr.ua/cgi-bin/koha/opac-detail.pl?biblionumber=8698

10. Буров Є. В. Комп'ютерні мережі : підручник. Львів : Магнолія 2006, 2025. 262 с. ISBN 966-8340-69-8. Режим доступу: https://opac.kntu.kr.ua/cgi-bin/koha/opac-detail.pl?biblionumber=8692

Допоміжна

1. Filippo Menczer, Santo Fortunato, Clayton A. Davis A First Course in Network Science. Cambridge University Press. 2020. 300 с.

2. Charles E. Spurgeon, Joann Zimmerman Ethernet: The Definitive Guide: Designing and Managing Local Area Networks. O'Reilly Media. 2014. 508 с.

3. David Malone, Niall Richard Murphy IPv6 Network Administration: Teaching the Turtle to Dance. O'Reilly Media. 2005. 306 с.

4. Dale Liu Cisco Router and Switch Forensics: Investigating and Analyzing Malicious Network Activity. Syngress. 2009. 504 с.

5. Gerry Howser Computer Networks and the Internet. Springer. 2020. 575 с.

6. Gary Donahue Network Warrior: Everything You Need to Know That Wasn't on the CCNA Exam. O'Reilly Media; Second edition. 2011. 783 с.

7. Scott Jernigan CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008) (CompTIA Network + All-In-One Exam Guide). McGraw Hill. 2022. 976 с.

8. Ramon Nastase Computer Networking: The Beginner’s guide for Mastering Computer Networking, the Internet and the OSI Model (Computer Networking Series Book 1). 2017. 188 с.

9. David L. Mills Computer Network Time Synchronization: The Network Time Protocol on Earth and in Space, Second Edition. CRC Press. 2016. 494 с.

10. Andrew Tanenbaum, David Wetherall Computer Networks, Global Edition 6th Edition. Pearson. 2021. 900 с.

11. Larry L. Peterson, Bruce S. Davie Computer Networks: A Systems Approach 6th Edition. Morgan Kaufmann; 6th edition. 2021. 848 с.
12. William Oettinger. Learn Computer Forensics: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence, 2nd Edition. Packt Publishing. 2022. 434 с.
13. Ric Messier Network Forensics 1st Edition. Wiley. 2017. 322 с.
14. Vinit Jain. Wireshark Fundamentals. Apress Media. 2022. 267 с.

Інформаційні ресурси

15. Курс «Комп'ютерні мережі» на сервері дистанційної освіта ЦНТУ. – URL: https://moodle.kntu.kr.ua/course/view.php?id=1035
16. ChatGPT: вебсервіс штучного інтелекту [Електронний ресурс]. Режим доступу: https://chatgpt.com
17. Perplexity AI: інструмент пошуку з підтримкою ШІ [Електронний ресурс]. Режим доступу: https://www.perplexity.ai
18. Gemini: сервіс штучного інтелекту від Google [Електронний ресурс]. Режим доступу: https://gemini.google.com
19. Copilot: сервіс штучного інтелекту від Microsoft [Електронний ресурс]. Режим доступу: https://copilot.microsoft.com
20. Онлайн-курси UDEMY. – URL: https://www.udemy.com/ –платформа онлайн-курсів різних IT тематик.
21. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/ – українська платформа безкоштовних онлайн-курсів
22. Онлайн-курси Coursera. – URL: https://www.coursera.org –платформа онлайн-курсів різних IT тематик.
23. https://habr.com – колективний блог з новинами та аналітичними статтями про інформаційні технології та програмування.
24. http://stackoverflow.com/ – система питань і відповідей для професійних програмістів та новачків у програмуванні.

25. https://dou.ua/ – український веб-сайт з елементами колективного блогу, створений для розповсюдження новин, аналітичних статей та свіжої інформації пов'язаної із інформаційними технологіями.
26. https://www.google.com/ – основна пошукова платформа.
27. https://www.youtube.com – Відеохостинг, що надає користувачам послуги зберігання, доставки та показу відео. На платформі розміщено багато курсів IT спрямованості.
28. https://biblprog.org.ua/ua/programming/ – каталог безкоштовних середовищ розроблення ПЗ.
29. Національна бібліотека України імені В. І. Вернадського: Електронні ресурси НБУВ [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/