Міністерство освіти і науки України
Національний університет водного господарства та природокористування
Кафедра автоматизації, електротехнічних та комп'ютерно-інтегрованих технологій

04-03-414М

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
з навчальної дисципліни
«Захист інформації та мережева безпека»
для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»
денної і заочної форм навчання

Рекомендовано науково – методичною радою з якості ННІЕАВГ
Протокол №3 від 26.11.2024 р.

Рівне – 2024

Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни «Захист інформації та мережева безпека» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» денної і заочної форм навчання [Електронне видання] / Наумчук О. М. – Рівне: НУВГП, 2024. – 83 с.

Укладач: Наумчук О. М., доцент кафедри автоматизації, електротехнічних та комп'ютерно-інтегрованих технологій.

Відповідальний за випуск: Древецький В. В., д.т.н., професор, завідувач кафедри автоматизації, електротехнічних та комп'ютерно-інтегрованих технологій.

Керівник освітньої програми «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»: Христюк А. О., к.т.н., доцент кафедри автоматизації, електротехнічних та комп'ютерно-інтегрованих технологій.

Зміст

Вступ

Сучасні системи автоматизації та робототехніки так само, як і інші потребують застосування технологій захисту інформації та мережевої безпеки. Набуття практичних навиків для захисту інформації є важливою частиною формування здобувачами вищої освіти сучасного рівня знань, умінь і навиків з цього питання. Даний лабораторний курс допоможе студентам навчитися організовувати безпеку комп'ютерних мереж, які застосовуються на сучасних промислових підприємствах різних галузей. Також, він сприятиме засвоєнню основних принципів розробки та використання сучасних технологій по захисту інформації з подальшим їх використанням у професійній діяльності.

У лабораторних роботах розглянуто особливості застосування різних технологій захисту використовуючи можливості мережевих Linux-подібних операційних систем та операційної системи Windows.

Лабораторна робота №1
Розробка проекту політики інформаційної безпеки та захисту інформації підприємства

Мета роботи

Ознайомитись із основними положеннями стандарту ISO/IEC 17799 «Управління інформаційною безпекою. Практичні правила». Навчитись розробляти політику безпеки організації та запропонувати практичні кроки по її реалізації.

Теоретичні відомості

Стандарт ISO/IEC 17799 «Управління інформаційною безпекою. Практичні правила» визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, відповідальність співробітників, використання оцінки ризиків і т.д. в контексті інформаційної безпеки. В процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої – скорочення матеріальних втрат, пов'язаних з порушенням інформаційної безпеки. Стандарт покликаний заощадити підприємству фінансові та матеріальні засоби.

ISO17799 - це модель системи управління підприємством щодо його інформаційної безпеки. Розроблений у ньому підхід ґрунтується на заходах, які направлені на організацію управління діяльністю підприємства. Він розроблений на основі досвіду різних організацій та дозволяє реалізувати та оцінити ефективність процедур управління безпекою, а також дає можливість встановити довірчі відносини між різними організаціями.

Даний документ можна використовувати як загальноприйнятий стандарт при встановленні ділових відносин між організаціями і при підписанні контрактів з субпідрядниками або впровадженні інформаційних систем та продуктів.

Метою інформаційної безпеки є — забезпечити безперебійну роботу організації і зведення до мінімуму збитків від подій, що загрожують безпеці. Управління інформаційною безпекою дає можливість колективно використовувати інформацію, забезпечуючи при цьому її захист та захист обчислювальних

ресурсів. Інформаційна безпека складається з трьох основних компонентів:

а) конфіденційність: захист конфіденційної інформації від несанкціонованого розкриття або перехоплення;

б) цілісність: забезпечення точності і повноти інформації і комп'ютерних програм;

в) доступність: забезпечення доступності інформації і життєво важливих сервісів для користувачів, коли це потрібно.

Інформація існує в різних формах. Її можна зберігати на носіях, передавати по мережах, роздруковувати або записувати на папері, а також озвучувати в розмовах. З погляду безпеки всі види інформації, включаючи: паперову документацію, бази даних, диски, флеш-носії, хмарне середовище, розмови та все інше, що використовується для передачі даних, знань та ідей, потребує належного захисту.

Інформація, яку використовують різні інформаційні системи і технології є цінним виробничим ресурсом організації. Її доступність, цілісність і конфіденційність може мати особливе значення для забезпечення: конкурентоспроможності, руху грошових коштів, рентабельності, відповідності правовим нормам і іміджу організації. Сучасні організації стикаються зі зростаючою загрозою порушення інформаційної безпеки, що походить від багатьох джерел. Інформаційним системам і мережам можуть загрожувати: комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, відмови у роботі та аварії. З'являються все нові загрози, здатні завдати значних збитків, наприклад сучасні комп'ютерні віруси або хакерські атаки.

Передбачається, що такі загрози інформаційній безпеці з часом стануть все більш поширенішими, небезпечнішими і витонченішими. Разом з тим, через зростаючу залежність організацій від інформаційних систем і сервісів, вони можуть стати вразливішими по відношенню до загроз порушення захисту. Розповсюдження комп'ютерних мереж надає нові можливості для несанкціонованого доступу до комп'ютерних систем, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості їх централізованого контролю.

Захисні заходи будуть значно дешевшими і ефективнішими, якщо вони будуть розроблятися ще на стадіях розробки та

проектування. Чим швидше організація почне застосовувати заходи по захисту своїх інформаційних систем, ресурсів, мереж та даних тим дешевими і ефективними буде їх використання.

У відповідності до стандарту ISO/IEC 17799 на підприємствах пропонується застосовувати практичні заходи, які необхідно описати у таких розділах:

1. Політика безпеки.
2. Організація захисту.
3. Класифікація ресурсів і їх контроль.
4. Безпека персоналу.
5. Фізична безпека і безпека навколишнього середовища.
6. Адміністрування комп'ютерних систем і обчислювальних мереж.
7. Управління доступом до систем.
8. Розробка і супровід інформаційних систем.
9. Планування безперебійної роботи організації.
10. Виконання вимог.

У цих розділах представлений набір заходів управління безпекою, які засновані на практичних аспектах по захисту інформації у відповідності до досвіду сучасних міжнародних організацій.

Застосування засобів управління безпекою. Предстаавлені заходи інформаційної безпеки потрібно застосовувати з урахуванням місцевих умов. Проте більшість заходів, представлені у даній послідовності широко застосовують багато організацій, а їх використання рекомендується для всіх ситуацій з врахуванням обмежень. Ці заходи є базовими щодо управління безпекою, оскільки всі вони в сукупності визначають базовий промисловий стандарт на підтримку режимів безпеки. При використанні деяких із заходів контролю, наприклад, шифрування даних, можуть використовуватися сучасні системи шифрування, але перед їх застосуванням необхідно оцінки ризики, щоб визначити, чи потрібні вони і яким чином їх реалізувати. Для забезпечення вищого рівня захисту особливо цінних ресурсів або забезпечення протидії високим рівням загроз порушення режиму безпеки, можуть бути використані інші заходи контролю, які виходять за рамки передбачених правил.

Основні заходи захисту інформації підприємства:

- розробка документу про політику інформаційної безпеки;
- розподіл обов'язків по забезпеченню інформаційної безпеки;
- навчання і підготовка персоналу для підтримки режиму інформаційної безпеки;
- повідомлення про випадки порушення захисту;
- засоби захисту від вірусів;
- планування безперебійної роботи організації;
- контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;
- захист документації організації;
- захист даних;
- відповідність політиці безпеки.

Сучасні підприємства вирішують цю проблему, розробляючи принципи інформаційної безпеки для відповідних відділів та груп співробітників, щоб забезпечити ефективніше функціонування технологій захисту інформації.

Політика інформаційної безпеки. Метою політики інформаційної безпеки є визначення особливостей і забезпечення у актуальному стані інформаційної безпеки організації і/або системи. Положення про політику безпеки повинне бути доведене до відома всіх співробітників організації та користувачів системи.

Положення про політику безпеки має містити:

1) визначення інформаційної безпеки, її цілі, область застосування, її значення та механізми колективного використання інформації;

2) основні положення щодо реалізації мети та принципів інформаційної безпеки;

3) роз'яснення конкретних заходів політики безпеки, принципів, стандартів і вимог до її дотримання, включаючи:
- виконання правових і договірних вимог;
- навчання персоналу правилам безпеки;
- попередження і виявлення вірусів;
- забезпечення безперебійної роботи організації.

4) визначення загальних і конкретних обов'язків по забезпеченню режиму інформаційної безпеки;

5) роз'яснення процесу повідомлення про події, що несуть загрозу безпеці.

Особливості створення та використання паролів. Користувачі повинні вибирати нестандартні паролі. Це означає, що паролі не повинні бути пов'язані із заняттями або особистим життям користувачів.

Наприклад, не можна використовувати як пароль номер власного автомобіля, власне ім'я та ім'я дружини або дитини, дату та рік народження, частину адреси та ін. Це не означає, що пароль не повинен бути просто словом із словника. Також, не варто використовувати відомі імена, географічні назви, технічні терміни і сленг. Якщо є відповідні системні програмні засоби для здійснення контролю надійності що призначаються користувачам паролів, то необхідно використовувати ці засоби для того, щоб заборонити користувачам вибір легко вгадуваних паролів.

Паролі не повинні зберігатися в доступній для читання формі в командних файлах, сценаріях автоматичної реєстрації, програмних макросах, на комп'ютерах з неконтрольованим доступом, а також в інших місцях, де не уповноважені особи можуть отримати доступ до них. Користувачі не повинні вибирати таку опцію конфігурації, як автоматичне збереження пароля.

Не можна записувати паролі і залишати ці записи в місцях, де до них можуть отримати доступ не уповноважені особи. Пароль повинен бути негайно змінений, якщо є підстави вважати, що цей пароль став відомий будь кому крім користувача.

Для прикладу розробки політики інформаційної безпеки підприємства потрібно визначити структуру комп'ютерної мережі (мереж) підприємства. Такий підхід дасть змогу точно визначити її технічні та програмні можливості, а також оцінити конкретні вразливості даної структури. Розглянемо структуру комп'ютерної мережі підприємства, яка представлена на структурній схемі (рис. 1).

Представлена комп'ютерна мережа є змішаною локально-глобальною мережою з обмежувальним механізмом (апаратно-технічний) у вигляді брандмауера. Віддалені офіси, які можуть бути розташовані у різних частинах країни, мають можливість користуватись головними серверами за наявності спеціального токену доступу. Засоби адміністрування та система управління

розташовані безпосередньо на головному сервері(ах) та мають можливість користуватися ними без токенів.

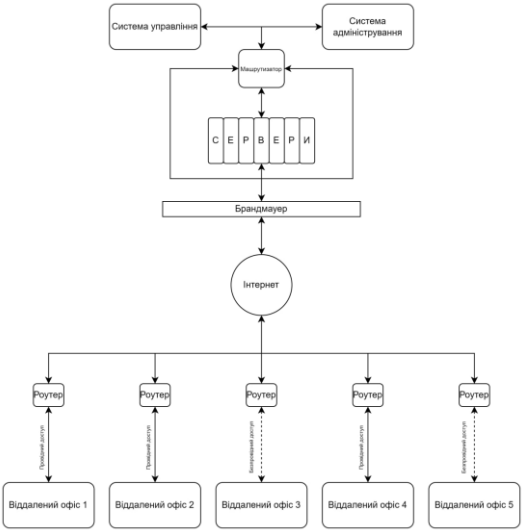

Рис. 1. Структурна схема комп’ютерної мережі підприємства

Серед вразливостей комп’ютерної мережі, які можуть виникнути в приведеній структурній схемі можуть бути такі:

• наявність помилок в програмному забезпеченні (ПЗ) та операційних системах (ОС);

• помилки адміністрування, конфігурації систем та методів захисту;

• невиконання рекомендацій спеціалістів по захисту мереж;

• економія на методах та системах безпеки чи ігнорування ними;

• недобросовістні працівники;

• несанкціонований доступ через недосконаліть локальних, безпроводових чи продових технологій зв’язку;

• обхід чи зламування головного захисту потоків даних до серверів у вигляді брандмауера;

• використання фейк-запитів до серверів з ціллю колекціонування обривків даних;

• DDoS-атаки з ціллю пошкодити комп’ютерну мережу;

• фізичні пошкодження (стихійні лиха, погодні катаклізми, неуважність працівників та ін.).

На відміну від структури комп'ютерної мережі інформаційна структура може суттєво відрізнятися і вона описує інформаційну взаємодію та обмін даними між окремими працівниками підприємства, або його відділами. Приклад інформаційної структури приведений на рис. 2.

Серед загроз інформаційної безпеки можуть виникати такі:

• використанні недосконалого ПЗ та неперевіреного обладнання;

• неповноцінні процеси роботи системи;

• складні експлуатаційних умови.

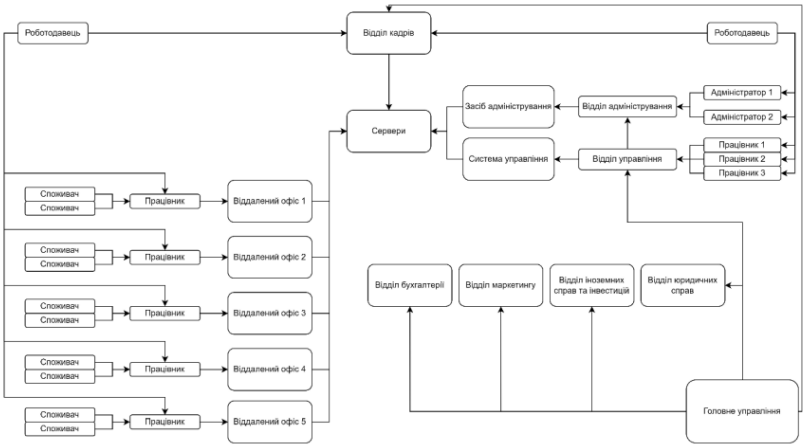

Рис. 2. Структурна схема інформаційної структури підприємства

Загрози інформаційної безпеки можуть мати організований та неорганізований (випадковий) характер. До ненавмисних загроз інформаційної безпеки відностяться:

• неполадки в роботі апаратури передачі даних;

• помилки та збої ПЗ;

• помилки в діях персонал або працівників, які працюють в системі;

• форс-мажори, викликані діями природних катаклізмів чи іншими непередбачуваними обставинами;

• проблеми через перебої електроенергії.

До навмисних загроз інформаційної безпеки відносяться:

• відсутність кібергігієни у працівників системи;
• використання публічних безпроводових точок доступу;
• надання токенів доступу для сторонніх користувачів;
• використання незареєстрованих у системі зовнішніх пристроїв;
• DdoS-атаки з ціллю пошкодити роботу системи;
• хакерські атаки з ціллю збору даних;
• порушення роботи брандмауера;
• підбір токенів доступу до системи;
• злиття даних працівником системи;
• імітація запитів до системи;
• обхід системи безпеки;
• ввід вірусів у систему.

Приведена технічна та інформаційна структура дозволить оцінити всі можливі вразливості та загрози і у майбутньому забезпечити мінімізацію наслідків від них.

Програма роботи

1. Розглянути основні положення стандарту ISO/IEC 17799 «Управління інформаційною безпекою. Практичні правила».
2. Навчитися розробляти політику безпеки організації.

Порядок виконання роботи

1. Розглянути структуру стандарту ISO/IEC 17799 та інформацію, яка приведена у теоретичних відомостях і на її основі розробити політику безпеки організації.

2. Вибрати організацію для розробки політики безпеки. У якості організації можна використати реальне підприємство з розвиненою структурою. Це може бути промислове підприємство, яке використовуватиметься у курсовій або бакалаврській роботі. Вибране підприємство повинно мати хоча б три відділи, наприклад: управління (керівництво), бухгалтерія, виробничий або транспортний відділи та ін. У ньому повинна функціонувати локальна комп'ютерна мережа (мережі) з головним сервером (серверами) і декількома частинами, які об'єднані мережевими маршрутизаторами, або іншим

обладнанням та виходом в інтернет.

3. Розробити блок-схему комп'ютерної мережі (мереж) підприємства з детальним визначенням її структури та описати її структуру (див. приклад на рис. 1).

4. Розробити блок-схему інформаційної структури вибраного підприємства з деталізацією його підрозділів і засобів, які у них використовуються та описати інформаційну структуру (див. приклад на рис. 2).

5. Визначити загрози інформаційної безпеки підприємства. Для цього оцінити всі вразливі місця комп'ютерної мережі (мереж) та будь-які інші вразливості, які можуть виникати при функціонуванні підприємства (використання безпроводових точок доступу, доступ сторонніх користувачів та ін.).

6. Розробити структуру захисту комп'ютерної мережі (мереж). Для цього потрібно запропонувати адміністративні, організаційні та програмно-технічні заходи щодо покращення рівня безпеки мережі. Наприклад, запровадження сучасного антивірусного захисту, ведення журналів подій, запровадження сучасних маршрутизаторів з підвищеним рівнем безпеки, введення систем шифрування даних, розмежування доступу та ін. Додайте конкретний перелік заходів.

7. Розробити структуру інформаційної безпеки підприємства у відповідності до встановлених у ISO/IEC 17799 розділів та обґрунтувати розроблену політику безпеки. У якості прикладу для розробки політики безпеки можна використовувати існуючі розробки реальних підприємств.

8. Результати роботи оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульна сторінка;
- мета роботи;
- порядок виконання роботи;
- опис усіх етапів виконання роботи;
- опис отриманих результатів;
- висновки за результатами роботи.

Контрольні запитання

1. Яке призначення стандарту ISO/IEC 17799?
2. В чому полягає зміст інформаційної безпеки?
3. Описати структуру стандарту ISO/IEC 17799.
4. Які засоби контролю використовуються при управлінні безпекою?
5. Які групи вимог до системи безпеки організації визначаються стандартом ISO/IEC 17799?
6. Які аспекти розглядаються при оцінці ризиків безпеки?
7. Які умови необхідно виконати для успішної реалізації системи інформаційної безпеки?
8. Яку інформацію повинен містити документ про політику інформаційної безпеки?
9. Описати структуру документу про політику інформаційної безпеки організації?

Лабораторна робота №2
Дослідження технологій поширення комп'ютерних вірусів та способів захисту інформації

Мета роботи

Ознайомитись з основними видами комп'ютерних вірусів, принципами їх роботи поширення і знищення. Розглянути програми для захисту від вірусів, принцип їх дії, ефективність та можливості.

Теоретичні відомості

Комп'ютерні віруси, їх властивості і класифікація. Властивості комп'ютерних вірусів вказують на те, що вони є певним класом комп'ютерних програм. Комп'ютерний вірус (далі вірус) - це програма, що має здатність самовідтворюватися. Така здатність притаманна всім типам комп'ютерних вірусів. Але не тільки віруси здатні до самовідтворення, будь яка операційна система та багато інших програм можуть створювати власні копії. Особливістю копіювання вірусів є їх не повне співпадіння з оригіналом, вони можуть суттєво відрізнятися від нього, або взагалі з ним не співпадати.

Також вірус не може існувати в «ізоляції» від інших програм, інформації про їх файлову структуру або про імена інших програм. Це відбувається через те, що комп'ютерні віруси, зазвичай, намагаються різними способами передати управління собі. На сьогодні відомі десятки тисяч комп'ютерних вірусів, які можна поділити на такі *види*:

1. *За середовищем розповсюдження*:

- завантажувальні віруси - це найбільш небезпечна група вірусів, що заражають Boot Record та Master Boot Record логічних та фізичних дисків;
- файлові віруси - це віруси, які поширюються, заражаючи файли різних типів, найчастіше це виконуючі файли. Сюди також відносять макровіруси, які деколи виділяють в окремий клас;
- завантажувально-файлові віруси - здатні вражати, як код завантажувальних секторів, так і код файлів, як правило системних;
- віруси сімейства Dir - використовують інформацію про

файлову структуру та вміст каталогів;

- multipartition – це віруси, які можуть вражати одночасно виконуючі файли, boot - сектори, MBR, FAT каталоги і є найбільш небезпечними, тому що вони часто мають поліаморфні властивості і елементи невидимості;

- мережеві віруси - це віруси, що поширюються у вигляді машинних кодів в комп'ютерних мережах;

- поштові віруси - дуже поширена група вірусів, що розповсюджуються разом з поштовими повідовленнями у вигляді прикріплених файлів (Attachment) з програмним кодом. Як правило, такі віруси досить швидко розмножуються і час від часу викликають вірусні епідемії.

2. *За алгоритмом роботи*:

- віруси "паразити" – це найпростіші віруси що використовують "тіло" інших файлів (виконуючих), записуючи туди себе. Вони можуть бути легко виявлені і знешкоджені;

- віруси супутники створюють копію exe-файлу з розширенням *.com і записують туди себе. Коли з командного рядка ОС завантажують такий файл, то як правило, розширення не вказують, але зазвичай, першим завантажується *-com файл, тобто вірус, який згодом швидко поширюється;

- віруси "черв'яки", або "хробаки" (віруси-реплікатори) поширюються в комп'ютерних мережах та в оперативній пам'яті ПК у вигляді певного машинного коду. Вони ніби черв'яки проникають в оперативну пам'ять ПК через комп'ютерну мережу, локалізуючи системи захисту. Найбільш небезпечними представниками цього типу вірусів є Nimda (неодноразовий переможець рейтингів найнебезпечніших вірусів), Gigger та Redesi (здатні відформатувати диск С), Bumerang (здатний знищити FlashBIOS та таблиці файлової системи жорстких дисків), SirCam (найдзвичано швидкий у розповсюдженні та знищує інформацію на диску С) та інші;

- студентські віруси - це віруси, які містять багато помилок і написані, як правило, початківцями;

- віруси "невидимки" (Stealth - віруси) фальсифікують інформацію, перехоплюючи звертання антивірусної програми, до заражених ділянок диску і направляючи її на незаражені. Ця технологія використовується, як у файлових, так і в

завантажувальних вірусах;

- віруси “мутанти” (“привиди”) або поліаморфні – не мають постійної сигнатури (машинного коду), за якою можна було б його виявити. Вони змінюють сигнатуру з кожною копією і тому з ними важко боротись. Виявляють такі віруси лише за допомогою евристичного аналізу, коли антивірусна програма прочитує алгоритм роботи виконуючих файлів і в разі підозрілих операцій ідентифікує його, як підозрілий об’єкт, тобто вірус. Саме таким чином антивірусні програми шукають ще невідомі їм віруси;

- ретровіруси - це звичайні файлові віруси, які намагаються заразити антивірусні програми, знищуючи, або роблячи їх непрацездатними, тому практично всі антивіруси в першу чергу перевіряють свої власні параметри і контрольні суми;

- “троянські” віруси (trojans) здійснюють шкідливі дії замість визначених легальних функцій або разом з ними. Вони переважно не здатні на саморозповсюдження і передаються тільки при їх копіюванні користувачем. Часто ці віруси використовують в якості “шпигунів”. Проникаючи по мережі на ПК, вони намагаються “затаїтись” і “викрасти” паролі користувача та передати їх власнику вірусa. Деякі троянські віруси готують заражені ними ПК для безперешкодного проникнення інших вірусів. Боротись з такими вірусами (особливо новими) дуже складно, адже в їх коді немає ніякої деструктивної дії (не міняється розмір файлів, не форматуються диски), а навпаки вони намагаються ніяк себе не проявити. Для боротьби з такими вірусами використовуються спеціальні мережеві екрани FireWoll (фаєрволи), які під час підключення до мережі слідкують чи не намагається якась програма самостійно передавати інформацію в Internet. Якщо така спроба відбулась, то вона блокується і виводиться повідомлення з запитом дозволу на таку операцію. Варто зауважити, що існує багато відомих троянських вірусів, які не лише виступають в ролі “шпигунів” але й самі несуть досить високу деструктивну дію (наприклад TROJ_ZERAF знищує exe і sys файли та утворює помилки в системному реєстрі);

- віруси таймери - очікують певного часу (певної години) і лише тоді спрацьовують.

3. *За деструктивною дією*:

- нешкідливі віруси - це віруси, які не приносять жодної шкоди, а просто себе копіюють багато разів, заповнюючи диски, або загромаджуючи оперативну пам'ять;

- не небезпечні віруси схожі до попередніх, але крім цього їх дія супроводжується різними спецефектами (відео та аудіо);

- небезпечні віруси - це віруси дія яких призводить до серйозних збоїв в роботі ПК, таких, як зависання, форматування, передача даних та ін.;

- дуже небезпечні віруси - це віруси, дія яких супроводжується знищенням інформації (файлів, каталогів, форматування дисків).

4. *За принципом дії*:

- резидентні - це віруси, що завантажуються в оперативну пам'ять і постійно там знаходяться, аж до виключення живлення чи перезавантаження ПК;

- не резидентні - це віруси, які короткочасно завантажуються в пам'ять, виконують потрібні їм дії і вивантажуються з пам'яті.

5. *За місцем додавання вірусу у файли*:

- на початку файлу;

- всередині файлу;

- в кінці файлу.

Види файлів, які можуть бути заражені вірусом. Як правило, кожна конкретна різновидність вірусу може заразити тільки один або два типи файлів. На даний час частіше всього зустрічаються макровіруси, тоді як раніше найпоширенішими були віруси, що заражали com та exe файли.

Види файлів, які можуть бути заражені вірусом:

- виконуючі файли, тобто файли з розширенням com та exe, а також файли, завантажені іншими програмами. Вірус в заражених ним виконуючих файлах починає свою діяльність при завантаженні тієї програми, в якій він знаходиться;

- файли документів та шаблонів, створених програмами Word, Excel, Access та іншими офісними програмами, а саме макроси, що використовуються у них. Цей тип вірусів порівняно новий і тому називається макровірусами. Деякі з вірусів цього типу є надзвичайно шкідливими. Наприклад, вірус W97M.Thus здатний знищити всі файли на диску C, зберігаючи при цьому структуру каталогів (папок);

- блок початкового завантаження операційної системи і головного завантажувального запису жорсткого диску. Вірус, який заразив ці ділянки, як правило, складається з 2-х частин, оскільки на цих ділянках диску складно розмістити цілу програму вірусу. Частина вірусу, що не поміщається в них, розташовується на іншій ділянці диску, який визначається, як дефектний. Такий вірус починає свою роботу при початковому завантажуванні операційної системи і є резидентним, тобто постійно знаходиться в пам'яті комп'ютера. Відомі випадки, коли вірус форматує додаткову частину диску, куди він записує основну частину програми;

- таблиці файлової системи та каталоги. Як відомо, в кожен каталог записуються імена файлів, дата та час створення, номер першого кластера файлу, а також резервні байти. Віруси цього типу, записавшись в кластери, помічають їх, як пошкоджені, а тоді реорганізовують файлову систему. При цьому інформація про перші кластери деяких виконуючих файлів записується у резервні біти, а на її місце поміщається посилання на тіло вірусу. Тому, при спробі користувача завантажити відповідну програму – вірус отримує спеціальне керівництво.

- драйвери пристроїв, тобто файли, які здійснюють програмне керування зовнішніми пристроями. Вірус, який знаходиться в цих файлах, починає свою роботу при кожному звертанні до відповідного пристрою;

- системні файли, тобто файли IO.SYS і MSDOS.SYS. Їх зараження досить небезпечно, оскільки вони, як і у випадку зараження блоків початкового завантаження дисків, починають діяти при кожному завантаженні ПК.

Шляхи проникнення вірусів в ПК. Яким чином комп'ютерний вірус може потрапити на ПК користувача? На початку існування вірусів основним середовищем їх розповсюдження були переносні диски, переважно дискети. Пізніше, CD та DVD-диски стали зручним середовищем поширення вірусів (перш за все не ліцензійні програмні продукти). Потім основним середовищем розповсюдження комп'ютерних вірусів стали комп'ютерні мережі та електронна пошта. Інтенсивний розвиток Internet сприяє можливості миттєвого поширення нових вірусів на дуже великі відстані та

території.

Варто пам'ятати проте, що розробники комп'ютерних вірусів постійно шукатимуть нові шляхи їх розповсюдження. Так, наприклад, відомі вже випадки поширення вірусів через файли в форматі RTF, PDF та анімаційні файли, створені в Macromedia Flash та інших мультимедійних програмах.

Захист від комп'ютерних вірусів. Для захисту від вірусів застосовують спеціалізовані програми. Ці програми поділяють на такі види:

- детектори - дозволяють знайти файли, заражені відомим вірусом;

- вакцини (імунізатори) - модифікують (інфікують) програми і диски таким чином, що це не відображається на їх роботі. Після цього вірус, від якого виконується вакцинація, вважає ці програми або диски інфікованими і повторно їх не заражає;

- лікарі (фаги) - лікують заражені програми або диски видаляючи із заражених програм тіло віруса, тобто відновлюючи програму в тому стані, в якому вона була до зараження вірусом;

- ревізори - спочатку запам'ятовують стан інформації (розмір, дату і час створення) і системних ділянок дисків, а потім порівнюють її з поточною. При виявленні невідповідностей повідомляють користувачу;

- лікарі-ревізори - це гібриди ревізорів і лікарів, тобто програми, які не тільки помічають зміни в файлах і системних ділянках дисків, але й можуть у випадку виявлення змін вилікувати заражені файли;

- фільтри (монітори) - резидентні програми для захисту від вірусів, які поміщаються резидентно в оперативній пам'яті комп'ютера і перехоплюють звернення вірусів до системних ділянок і файлів. Користувач може дозволити або заборонити виконання відповідних операцій;

- поліфаги - це найефективніша група програм, що поєднують в собі декілька типів антивірусів, наприклад, фільтрів, детекторів та лікарів.

Сьогодні багато компаній займаються розробкою нових та ефективних програм для захисту ПК від вірусів. Найбільш авторитетним показником ефективності антивірусних програм є рейтинг, який щомісяця проводить міжнародний комп'ютерний

журнал Virus Bulettin (https://www.virusbulletin.com). Також регулярно проводяться тестування, при яких антивірусні програми встановлюються в однакових умовах на заражені різними типами вірусів комп'ютери і визначається відсоток виявлених та знешкоджених ними вірусів. Тестування проводиться за категоріями: макровіруси, поліморфні віруси та стандартні віруси. При тестуванні антивірусних програм враховуються також такі параметри як швидкість роботи програми, її вартість та зручність інтерфейсу. Сама участь антивірусної програми в тестуванні вказує на її достатньо високу ефективність.

Антивірусний захист в ОС Windows 10 за допомогою служби "Безпека у Windows". Служба "*Безпека у Windows*", забезпечує повний захист ПК з моменту запуску Windows 10. Програма "Безпека у Windows" постійно перевіряє систему на наявність шкідливих програм, вірусів та інших загроз безпеки. Крім цього, в реальному часі, автоматично завантажуються оновлення, щоб ПК залишався безпечним і захищеним від найновіших загроз "Безпека у Windows" вбудовано в ОС Windows 10 містить програму захисту від вірусів (Антивірус) Microsoft Defender.

Microsoft Defender – це безкоштовне програмне забезпечення для захисту від зловмисних програм, яке входить до складу Windows, і воно оновлюється автоматично через Windows Update. Microsoft Defender здійснює виявлення загроз в реальному часі, а також містить брандмауер і функції батьківського контролю. Ця програма встановлюється в ОС Windows 11, 10, 8 і 7.

Програма Windows Defender надає два способи запобігання інфікуванню ПК:

1. Захист у реальному часі. Windows Defender попереджає, коли шпигунська програма намагається інсталювати або запустити себе на комп'ютері, а також активується, коли програми намагаються змінити важливі настройки ОС Windows.

2. Параметри сканування. За допомогою Windows Defender можна шукати на комп'ютері шпигунські програми, регулярно сканувати й видаляти всі відомі види вірусів знайдені під час сканування.

Служба “Безпека у Windows” (або “Центр безпеки для Захисника Windows” у попередніх версіях Windows) виявляє небезпечні та високостійкі зловмисні програми на ПК і видає повідомлення про те, що зловмисне програмне забезпечення знайдено на ПК, або повідомляє про те, що потрібно додаткове очищення.

У випадку підозри наявності на ПК зловмисного програмного забезпечення можна примусово запустити сканування за допомогою Microsoft Defender з меню настройок служби “Безпека у Windows” за приведеною послідовністю: *Кнопка Пуск > Параметри (Налаштування) > Оновлення та захист > Безпека у Windows > Захист від вірусів і загроз*.

Крім іншого, у закладці “Безпека у Windows” (рис. 1) є можливість настроїти різні елементи захисту ПК та налаштувати їх за вимогами користувача.

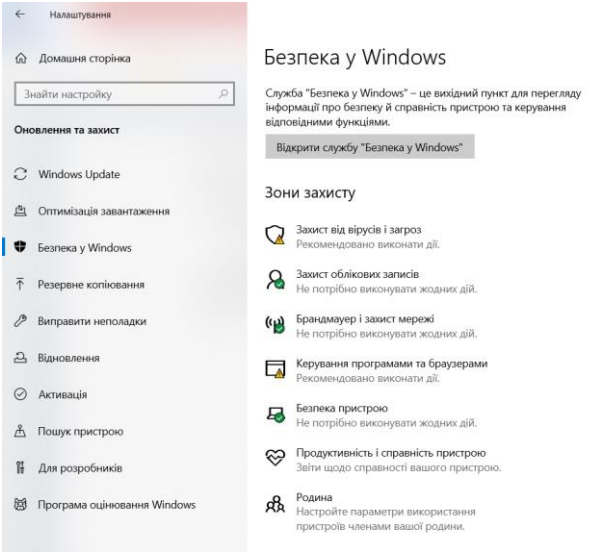

Рис. 1. Елементи настроювання служби “Безпека у Windows”

За допомогою зміни параметрів у вкладці служб “Безпека у Windows” можливо виконати настроювання кожної служби окремо під особливі вимоги користувача і забезпечити

відповідний рівень захисту та безпеки.

Служба “Безпека у Windows” — це вихідний пункт для перегляду інформації про безпеку й справність пристрою та керування відповідними функціями. Вона містить наступний функціонал (Рис. 2):

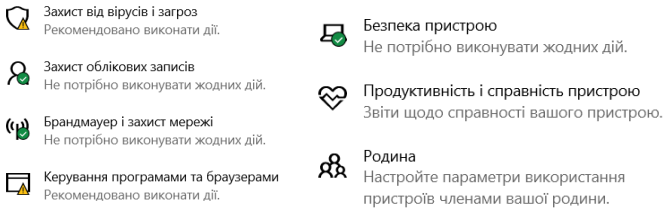

Рис. 2. Зони захисту ОС у службі “Безпека у Windows”

Елементи вкладок служби “Безпека у Windows”:

• *Захист від вірусів і загроз* — це захист пристрою від загроз. Вона може перевірити файли на рахунок вірусів та допомогти їх знищити. Є можливість налаштувати час, коли служба автоматично почне сканування.

• *Захист облікових записів* — це безпека облікового запису та вхід. Допомагає налаштувати вхід в систему, використовуючи аккаунт Microsoft. Можна ввімкнути динамічне блокування — спосіб входу в ОС: ключ безпеки, пароль, графічний пароль, відбиток пальця, або сканування обличчя.

• *Брандмауер і захист мережі* — хто й що може отримувати доступ до мережі. Можна налаштувати мережу домену, приватну або загальнодоступну мережу.

• *Керування програмами та браузерами* — захист програм та безпека в інтернеті. Є можливість ввімкнути захист на основі репутації, ізольований перегляд веб сторінок, запобігання експлойтам.

• *Безпека пристрою* — ізоляція ядра (захист основних компонентів пристрою), процесор безпеки (додаткове шифрування пристрою), безпечне завантаження (захист від завантаження зловмисних програм).

• *Продуктивність і справність пристрою* — можна переглянути звіти щодо справності пристрою.

• *Родина* — батьківський контроль

У результаті швидкої перевірки, якщо з антивірусною безпекою все добре, то отримаємо таке повідомлення (рис. 3):

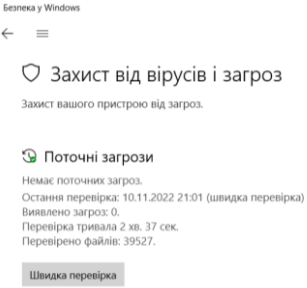

Рис. 3. Результати швидкої перевірки на наявність загроз

Програма роботи

1. Розглянути основні типи вірусів та програм, які їх знешкоджують.
2. Навчитися налаштовувати службу “Безпека у Windows” та ефективної використовувати для захисту ПК.

Порядок виконання роботи.

1. Ознайомитись з основними типами вірусів, технологіями їх поширення та захисту, а також зі службою ***“****Безпека у Windows”* з теоретичних відомостей.
2. З доступних у мережі інтернет відкритих джерел, наприклад Virus Bulettin (https://www.virusbulletin.com) та інших ознайомитися з поширеними вірусами.
3. Вибрати по одному з існуючих типів вірусів (макровіруси, поліморфні віруси, стандартні віруси) та:

3.1. Розглянути принцип роботи даного типу вірусів;

3.2. Навести назви вірусів даного типу (підвиди, сімейства) та описати методи їх поширення;

3.3. Розглянути програми та методи, які використовують для знищення даного типу вірусів;

4. Проаналізувати особливість роботи служби “Безпека у Windows”.
5. Провести настроювання елементів вкладок служби “Безпека у Windows” на ПК.
6. Настроїти та оцінити рівень захисту ПК (ОС Windows 10)

7. Результати роботи оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму та порядок виконання роботи;
- скріншоти з типами вірусів, технологіями їх поширення та захисту (п. 3);
- скріншоти з особливістю роботи служби “Безпека у Windows” (пп. 4-6).
- висновок.

Контрольні запитання

1. Що таке комп’ютерний вірус?
2. Класифікація комп’ютерних вірусів.
3. Опишіть класифікацію комп’ютерних вірусів за алгоритмом роботи.
4. Опишіть класифікацію комп’ютерних вірусів за деструктивною дією.
5. Опишіть класифікацію комп’ютерних вірусів за принципом дії та за місцем втілення вірусу у файли.
6. Опишіть види файлів, які можуть бути заражені вірусом.
7. Опишіть технології захисту від вірусів, які застосовують спеціалізовані програми.
8. Опишіть особливість служби “Безпека у Windows” в ОС Windows 10.

Лабораторна робота №3
Використання віртуалізації, DHCP та DNS-серверів

Мета роботи

Ознайомитись з можливостями віртуалізації VirtualBox. Вивчити способи отримання IP-адреси вузлів та навчитись використовувати DHCP-клієнт та налаштовувати DHCP та DNS-серевер.

Теоретичні відомості

Віртуалізація – надання абстрагованих від апаратної реалізації обчислювальних ресурсів, що забезпечує логічну ізоляцію процесів, виконуваних на одному фізичному ресурсі. Віртуалізація дозволяє запустити декілька операційних систем (ОС) на одному комп'ютері. За допомогою цієї властивості можна убезпечити операційну системи та ПК від помилок та пошкоджень на етапі розробки і впровадження нових операційних систем, програм та функцій, а також для безпечного використання мережевих функцій та налаштувань.

Поширеним способом віртуалізації є бінарна трансляція, що полягає у перехопленні гіпервізором інструкцій віртуалізованої системи та їх заміні на "безпечні" інструкції, що далі виконуються процесором (напр., VMWare Workstation, VirtualBox, QEMU). Гіпервізор – це програма, яка керує фізичними ресурсами обчислювальної машини та розподіляє ці ресурси між декількома різними операційними системами, дозволяючи запускати їх одночасно.

Більшу продуктивність віртуалізовних систем забезпечує паравіртуалізація («спосіб свідомого співробітництва»), гостьові операційні системи підготовлюються для виконання в віртуалізованому середовищі, для чого програмне ядро цих операційних систем дещо модифікується. Операційна система взаємодіє із програмою гіпервізора, який надає їй гостьовий API, замість використання безпосередньо таких ресурсів, як таблиця сторінок пам'яті.

Апаратна віртуалізація – віртуалізація за допомогою спеціальної процесорної архітектури. На відміну від програмної віртуалізації, можливе використання ізольованих гостьових

систем, керованих гіпервізором безпосередньо. Апаратна віртуалізація забезпечує більшу продуктивність у порівнянні з продуктивністю невіртуалізованної машини, що дає віртуалізації можливість практичного використання і широкого застосування. Найбільш поширені технології віртуалізації Intel-VT і AMD-V (Xen, VMWare Workstation, VirtualBox).

DHCP (Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла) — це протокол прикладного рівня моделі OSI, що дозволяє комп'ютерам підключеним до мережі автоматично одержувати IP-адресу та інші параметри, необхідні для роботи в мережі. Для цього комп'ютер звертається до спеціального серверу DHCP. Під час запуску системи комп'ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення-відповідь, яка містить IP-адресу і деякі інші конфігураційні параметри. При цьому сервер DHCP може працювати в різних режимах:

Динамічний розподіл. Адміністратор присвоює IP-діапазон адрес на сервері DHCP. Кожен клієнтський комп'ютер в мережі повинен запитати IP-адресу від DHCP-сервера, коли мережа ініціалізується за концепцією "оренди". Коли закінчується термін оренди, якщо вона не буде продовжена, DHCP-сервер має право повернути адресу і призначити її на інші комп'ютери.

Автоматичне виділення. Сервер DHCP буде постійно призначати вільну IP-адресу з діапазону, встановленого адміністратором, запитуючому комп'ютеру. Основна відмінність з динамічним розподілом в тому, що сервер зберігає записи минулих оренд і намагається привласнити ту ж адресу тому ж комп'ютеру для майбутніх мережних підключень.

Статичний розподіл. Сервер DHCP здійснює призначення IP-адрес виключно на основі таблиці MAC-адрес, які зазвичай заповнені вручну адміністратором мережі. Якщо MAC-адреса комп'ютера не зазначена в таблиці, йому не буде призначена мережева адреса.

NAT (від англ. Network Address Translation — «перетворення мережевих адрес») — це механізм у мережах TCP/IP, який дозволяє змінювати IP-адресу у заголовку пакету, що проходить через пристрій маршрутизації трафіку.

DNS (Domain Name System) — ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу. Розрізняють декілька типів процедур перетворення DNS імен. Серед них найбільшого поширення здобули рекурсивна та нерекурсивна процедури.

Особливість нерекурсивної процедури запиту DNS імен:

1) DNS-клієнт звертається до кореневого DNS-сервера з вказівкою повного доменного імені;

2) DNS-сервер відповідає клієнту, вказуючи адресу наступного DNS-сервера, який виконує обслуговування домену верхнього рівня, заданого в наступній старшій частині імені;

3) DNS-клієнт виконує запит наступного DNS-сервера, який його надсилає до DNS-сервера потрібного піддомена і т.д., доти, доки не буде знайдено DNS-сервер, який повністю відповідає запитуваному імені IP-адреси. Сервер дає кінцеву відповідь клієнту.

Особливість рекурсивної процедура:

1) DNS-клієнт запитує локальний DNS-сервер, який обслуговує піддомен, якому належить клієнт;

2) якщо локальний DNS-сервер відповідь знає, то повертає її клієнту, в протилежному випадку виконує ітеративні запити до кореневого сервера до тих пір, поки не отримає відповідь;

3) після отримання відповіді сервер передає її клієнту.

Таким чином, при рекурсивній процедурі клієнт фактично передоручає роботу власному серверу. Для прискорення пошуку IP-адрес DNS-сервери часто застосовують кешування відповідей, які проходять через них.

Для виконання різноманітних операцій та команд з адміністрування та захисту комп'ютерних мереж широко використовуються Unix-подібні операційні системи. Одна з таких – Linux. Linux є розробкою вільного програмного забезпечення. На відміну від комерційних операційних систем (Microsoft Windows та MacOS), початкові коди Linux доступні усім для використання, зміни та розповсюдження абсолютно вільно (в тому числі безкоштовно).

Система Linux спочатку розроблена для використання на персональних комп'ютерах, але пізніше вона набула популярності, як серверна операційна система (компанії, що

надають послуги вебхостингу, використовують Linux на своїх вебсерверах).

Типовий дистрибутив Linux складається з:

- ядра Linux;
- інструментів та бібліотек проєкту GNU;
- додаткових програм;
- документації;
- графічної системи (графічного серверу);
- віконуваного менеджера;
- середовища робочого столу та ін.

Сьогодні існує велика кількість дистрибутивів Linux, які використовуються, як у вбудованих системах так і мають спеціалізоване призначення. Серед них: Ubuntu, Debian, Linux Mint, CentOS, openSUSE, Fedora та інші.

Сучасні системи Linux дозволяють виконувати практично все за допомогою програм з графічним інтерфейсом, починаючи від встановлення програмного забезпечення і закінчуючи налаштуванням системи. Але для роботи з серверами, адмініструванням мереж та для інших задач теж використовується термінал. Термінал - це програма Linux, яка має інтерфейс командного рядка і є інструментом, за допомогою якого здійснюється керування операційною системою та виконання багатьох різноманітних операцій. За допомогою термінала можна: встановлювати і запускати програми; працювати з файлами; налаштовувати систему та багато іншого. Для роботи в терміналі необхідно використовувати команди. Команда - це ім’я програми, яке вводиться в терміналі для її запуску. Разом з ім’ям в команді можуть бути присутніми опції і параметри.

У нашому випадку ми використовуватимемо команди дистрибутива Debian. Варто зауважити, що тіж команди використовуються та подібні для інших дистрибутивів Linux. Розглянемо деякі приклади команд терміналу:

lsb_release -a виводить інформацію про поточну версію ОС;

uname -a надає інформацію про поточне ядро системи;

su (англ. “substitute user” - замінити користувача) застосовується для перемикання з одного користувача на іншого, при цьому вона може запустити як оболонку входу в умовах поточного каталогу і оточення (su), так і повністю змінити

налаштування, замінивши їх оточенням цільового користувача (su -). Синтаксис команди: *su [ім'я_користувача]*;

sudo (англ. “Substitute User and do“ - підмінити користувача та виконати) використовується як префікс до команд Linux, дозволяючи користувачеві виконувати команди, що вимагають привілеїв *root*.

На відміну від *su*, команда *sudo* вимагає введення пароля поточного користувача. *root* або суперкористувач — це спеціальний обліковий запис та група користувачів у Unix-подібних системах з ідентифікатором, власник якого має право на виконання всіх без винятку операцій. З іншими командами можна познайомитися у документації до дистрибутива, а також на різноманітних довідкових ресурсах наприклад: *https://linuxguide.rozh2sch.org.ua*

Програма роботи

1. Створити віртуальну машину та ознайомитись з її інтерфейсом.
2. Запустити віртуальну машину та встановити операційну систему Debian.
3. Переглянути налаштування мережі гостьової системи: отриману IP-адресу та адресу DNS-сервера, змінити тип підключення гостьової системи до локальної мережі та порівняти зміни в адресах.
4. Налаштувати та запустити DNS та DHCP-сервер у віртуальній машині.

Порядок виконання роботи

1. Запустити віртуальну машину Oracle VM VirtualBox.

Зауваження. Для роботи Oracle VM VirtualBox необхідно, щоб в налаштуванні BIOS було увімкнено апартну віртуалізацію на ПК. Якщо процесор ПК не підтримує апаратну віртуалізацію AMD-V або Intel VT-x необхідно в налаштуваннях віртуальної машини зняти відмітку «*Увімкнути VT-x/AMD-V*» на вкладці *Система > Прискорення*.

2. Скопіювати файл віртуального диска на локальний комп’ютер.
3. Створити нову віртуальну машину (кнопка

Create/Створити на панелі інструментів). Вибір операційної системи у вікні створення впливає лише на відображувану піктограму створеної віртуальної машини та не обмежує використання у віртуальній машині інших операційних систем, наприклад, Windows (у нашому випадку вказуємо тип Debian).

4. Вказати розмір RAM не менше ніж 512 Мб.

5. Створити новий віртуальний диск, прийнявши параметри за замовчуванням. Підключаємо ISO-образ інсталяційного диску з якого буде встановлюватися операційна система та вказуємо шлях до папки з попередньо завантаженою інсталяцією операційної системи. У нашому випадку це ОС Debian з ядром Linux. Установочний ISO-образ завантажуємо за посиланням *https://www.debian.org/download*. За вказаним посиланням знаходиться найновіший iso-образ ОС Debian. На момент виходу даних методичних вказівок - debian-12.7.0.

Для запуску інсталяції потрібно в *Налаштування* віртуальної машини у закладці *Пам'ять* додати *Оптичний привід* у який треба додати попередньо завантажений ISO-образ Debian 12. У процесі встановлення вказуємо логін і пароль для звичайного користувача та користувача з правами адміністратора, тобто *root*, а також інші параметри операційної системи. Після встановлення ОС Debian вимикаємо віртуальну машину.

6. Для повторного запуску віртуальної машини, якщо ОС Debian не запуститься автоматично, потрібно в меню *Пам'ять* вибрати встановлену операційну систему та за допомогою опції налаштування (кнопка *Налаштувати*) задаємо тип підключення до мережі — *проміжний адаптер/мережевий міст*.

7. Знову запускаємо віртуальну машину. Входимо в систему з логіном та паролем вказаними при встановленні операційної системи.

Зауваження. Для виконання команд у ОС Debian необхідно серед доступних програм вибрати *Термінал,* після цього можна виконувати всі необхідні процедури та команди.

8. Виконати команду *sudo ip a* (*sudo* – виконати від імені іншого користувача, за замовчуванням – суперкористувач *root*, *ip* – налаштування інтерфейсу, ключ *a* – показати всі) та скопіювати результат у звіт. Вимкнути машину.

Зауваження. Якщо вхід в операційну систему здійснено під

користувачем *root*, то команду *sudo* можна не застосувати, а виконати команду *ip a*. Для переходу до користувача *root* потрібно виконати команду *su root* та після цього ввести пароль користувача root.

9. Змінити *налаштування мережі* у Oracle VM VirtualBox гостьової системи на NAT. Для цього необхідно пройти за вказаним шляхом (*Машина > Налаштувати > Мережа > Тип підключения > NAT*) та виконати зміни.

10. Порівняти отримані IP-адреси операційної системи Debian, яка запущена з віртуальної машини з адресою хост-системи, тобто з ОС Windows за допомогою команди *ipconfig -a*. Ці адреси мають належати до однієї підмережі.

11. Перевірити час передачі пакетів до вузла en.wikipedia.org програмою ping: *ping en.wikipedia.org*.

12. Перевірити час передачі пакетів до будь якого вузла вказавши його IP-адресу. Виконати команду *ping* в ОС Windows та порівняти дані з її виконанням в ОС Debian. Для зупинки виконання команди *ping* використати комбінацію CTRL+C.

13. Встановити *dnsmasq* та файловий менеджер Midnight Commander (MC) за допомогою команди *apt install dnsmasq mc*. Відкрити файл налаштування DHCP та DNS-сервера *dnsmasq* (файл знаходиться в каталозі */etc*, назва файлу: *dnsmasq.conf*). Змінити діапазон видаваних IP-адрес. Прив'язати MAC-адресу одного з хостів до IP-адреси. Для цього скористайтесь файловим менеджером MC та редактором *Nano*. Оскільки редагування файлів налаштувань дозволено лише користувачу *root* (суперкористувачу), запуск файлового менеджера здійснюється командою *sudo mc* (відповідно без *sudo*, якщо ви працюєте під користувачем *root*). Навігація по об'єктам у каталозі здійснюється клавішами керування курсором, перехід у батьківський каталог (на рівень вище) – вибором *.. (дві крапки)*, перегляд текстового файлу – натисканням F3, редагування – F4. При першій спробі редагування з *mc* буде запропоновано обрати текстовий редактор за замовчуванням. Рекомендується обрати *Nano* вибором відповідної цифри та натисканням Enter. Діапазон IP-адрес до видачі задається рядком *dhcp-range=*. За замовчуванням ці рядки закоментовані (починаються з '#' - символу коментаря та ніяк не інтерпретуються при зчитуванні налаштувань). Знайдіть і

розкоментуйте рядок (видаливши символ #), задайте діапазон адрес від 192.168.45.12 до 192.168.45.67 та час оренди 72 години. Аналогічно виконайте налаштування прив'язки IP-адреси до MAC-адреси, яке виконується подібним чином, знайшовши рядок виду: *#dhcp-host=MAC-адреса,IP-адреса*. Щоб зберегти внесені зміни, натисніть *Ctrl+O* та підтвердіть ім'я файлу для збереження натисканням Enter.

14. Вийдіть з текстового редактора натисканням *Ctrl+X* та з файлового менеджера натисканням *F10*. Для застосування нових налаштувань перезапустіть *Dnsmasq* командою *sudo service dnsmasq restart* (відповідно без sudo, якщо ви працюєте під користувачем *root*).

Зауваження. Виконавши пп. 13 і 14 ми налаштували можливість отримання іншими вузлами мережі IP-адрес, зокрема з прив'язкою MAC-адрес, що обмежує доступ інших комп'ютерів з невказаними нами MAC-адресами.

15. Результати виконання оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму та порядок виконання роботи;
- скріншоти з налаштуваннями створеної віртуальної машини;
- скріншоти з отриманими IP-адресами при використанні: *проміжний адаптер/мережевий міст* та *NAT*;
- скріншот файлу налаштувань *dnsmasq*;
- висновок, що пояснює різницю між отриманими адресами з та без використання NAT.

Контрольні запитання

1. Назвіть поширені технології апаратної віртуалізації.
2. Яка відмінність паравіртуалізації від повної віртуалізації?
3. Яке призначення протоколу DHCP?
4. Яка особливість операційної системи Linux?
5. Як і які основні команди використовуються в терміналі операційної системи Linux?

6. В чому різниця в роботі DHCP-серверів, налаштованих на статичний та динамічний розподіл адрес?

7. Яке призначення DNS?

8. Для чого використовують DNS-кешування?

Лабораторна робота №4
Резервне копіювання та відновлення даних

Мета роботи

Навчитись захищати інформацію використовуючи засоби резервного копіювання жорсткого диска та відновлювати дані з резервної копії.

Теоретичні відомості

Сучасні системи резервного копіювання інформації передбачають ефективну стратегію, організаційні рішення і політику збереження даних. Існують різні технології резервного копіювання, які відрізняються витратами коштів і часу:

- *повне резервне копіювання* — вибрані дані будуть скопійовані повністю. Найнадійніший спосіб, але потребує найбільшої кількості ресурсів, місця для зберігання даних і часу копіювання, тому в такому вигляді застосовується рідко, зазвичай комбінується з іншими видами. Дозволяє відновити втрачені дані з нуля швидше за всі інші види копіювання;

- інкрементне копіювання — записуються тільки ті дані, які були змінені з часу минулого копіювання. Для таких копій потрібно значно менше пам'яті, ніж при повному копіюванні і записуються вони значно швидше. При такому підході також необхідно періодично робити повну резервну копію, при будь-якій аварії систему відновлюють з такої копії, а потім накочуються на неї всі наступні інкрементні копії в хронологічному порядку. Важливим елементом інкрементного копіювання є відновлення видалених файлів і проміжних версій, які змінювалися;

- диференціальне резервне копіювання — схоже на інкрементне, тобто копіюються тільки зміни, зроблені з моменту останнього повного копіювання. Його відмінність полягає в тому, що в кожну наступну копію зберігаються зміни з попередньої і додаються нові. Для відновлення після аварії знадобиться тільки повна копія і остання з диференціальних, що значно скорочує час відновлення.

Створення резервної копії (*backup*) даних надає можливість виконати відновлення інформації при втраті оригіналу, з якого

було створено резервну копію. При цьому під втратою треба розуміти настання події, що призвела до зміни даних, після чого вони втратили цінність або були видалені з носія. Приклад: умисне завдання шкоди через видалення важливої для підприємства інформації.

Об'єкти резервного копіювання — це дані або сукупність даних, з яких можна створити резервну копію. Приклади об'єктів: файли або теки, дані прикладних програм, дані операційної системи чи сама ОС, образи віртуальних машин та дисків віртуальних машин, файлові системи тощо.

Рівні резервного копіювання. *Повне резервне копіювання* (Full Backup або L0) — повна копія даних. Рівень, який забезпечує створення повної копії об'єкту резервного копіювання. Цей рівень дозволяє забезпечити максимальну відповідність оригіналу даних його копії.

Диференційне резервне копіювання (Differential Backup або L1) — копіювання змін, що були зроблені після створення останньої повної копії. Створення такої копії потребує більше часу та займає більший об'єм, ніж додаткове копіювання, але дозволяє пришвидшити процес відновлення. Загалом є альтернативою між створенням повної або додаткової копії.

Додаткове резервне копіювання (Incremental Backup або L2) — копіювання змін, що відбулись із часу повного, диференційного або додаткового копіювання. Загалом на додаткове копіювання затрачається менше часу, бо копіюється менше файлів. Однак процес відновлення даних займає більше часу, оскільки повинні спочатку відновлюватися дані останньої повної копії і після цього - всі резервні копії, від яких залежить додаткова копія.

Під час роботи операційної системи деякі файли можуть використовуватись нею та бути недоступними для читання користувачем, тому резервна копія системного розділу ОС повинна виконуватись при неактивній ОС або використовувати технології ОС, що забезпечують актуальність вмісту файлів (Shadow Copy, Snapshot).

Щоб забезпечити можливість відновлення системного розділу у випадку, коли операційна система не може завантажитись з нього, резервну копію створюють за допомогою технологій LiveCD/LiveUSB/PXE. Це дозволяє за критичної помилки

завантаження операційної системи завантажити «рятувальний» LiveCD/LiveUSB/PXE та відновити вміст системного розділу. Лазерний диск, що дозволяє завантажити операційну систему з нього без необхідності встановлення, називають LiveCD. Якщо аналогічну функцію має USB-накопичувач, його називають LiveUSB. PXE (англ. Preboot Execution Environment) — середовище для завантаження комп'ютерів за допомогою мережевої карти без використання жорстких дисків, компакт-дисків чи інших пристроїв, що застосовуються при локальному завантаженні операційної системи. Для організації завантаження системи в PXE використовуються протоколи IP, UDP, DHCP та TFTP. PXE-код, який зазвичай знаходиться в ПЗП мережевої карти, отримує з мережі по протоколу TFTP (отримаючи для цього адресу TFTP-сервера за допомогою DHCP) виконуваний файл, після чого передає йому управління.

Як правило, резервну копію зберігають в файлі-образі диска. Образ диска — файл, що містить у собі повну копію вмісту та структури файлової системи та даних, що містяться на диску. Образ розділу диску бажано розміщувати на іншому фізичному носії, щоб у випадку виходу з ладу диску не був втрачений і образ диску.

Програма роботи

1. Ознайомитися з технологіями захисту даних за допомогою резервного копіювання з теоретичних відомостей.
2. Завантажити Live-CD з засобом резервного копіювання HDD та виконати резервне копіювання диска.
3. Відформатувати віртуальний диск та відновити дані з резервної копії.

Порядок виконання роботи

1. Скопіювати програми Clonezilla Live та GParted на локальний ПК відповідно з *https://clonezilla.org/downloads.php* та *https://gparted.org/download.php,* при цьому потрібно скопіювати образ у форматі *iso* з необхідними параметрами системи.

2. У віртуальній машині OracleVM VirtualBox створити новий жорсткий диск. Для цього у OracleVM VirtualBox Менеджер необхідно вибрати пункт: *Налаштування > Пам'ять >*

Контролер:SATA > Жорсткий диск натиснувши відповідну кнопку, яка *Додає жорсткий диск* (праворуч від меню *«Контролер: SATA»)*. Після цього під'єднуємо до віртуальної машини ISO-образ GParted та завантажуємося з нього натиснувши відповідну кнопку, яка *Додає привод оптичного диску* (праворуч від меню *«Контролер: IDE»)*. Після завантаження GParted у списку доступних жорстких дисків (у правому верхньому куті менеджера GParted натискаємо кнопку) вибираємо порожній жорсткий диск (як правило цей диск буде відображатися, як «не розподілено»). Виконуємо форматування цього нового жорсткого диску у файловій системі *ext4*. Для цього у меню *Пристрій* вибираємо *Створити таблицю розділів* тип таблиці *msdos*. Під час створення розділу (резервний диск) необхідно задати йому *мітку розділу*, у відповідному вікні, за допомогою якої його можна буде відрізнити при створенні резервної копії (якщо цю опцію не виконати, то відрізнити новий диск від існуючого буде складно). Після цього створюємо новий розділ (клацнувши по диску правою клавішею) і застосовуємо зміни.

3. Перезавантажити віртуальну машину та завантажитись з *Live CD Clonezilla*. Для цього у меню віртуальної машини у пункті: *Налаштування > Пам'ять > Контролер:IDE > Оптичний привід* вказати шлях до завантаженого *iso*-образу *Clonezilla* (див. п. 1). Запускаємо віртуальну машину і обираємо подальші налаштування *Live CD Clonezilla* за замовчуванням. Після виконання аналізу дискового простору ми отримаємо два диска, один з яких має встановлену операційну систему, а інший резервний. Обираємо другий диск на який буде виконуватися резервне копіювання.

Виконуємо резервне копіювання одного жорсткого диска в образ диска на іншому, використовуючи вказівки Clonezilla. Для кращого розуміння інтерфейсу при встановленні вибираємо українську або російську мову. Після запуску вибираємо роботу з дисками або розділами використовуючи образи, так як показано на рис. 1.

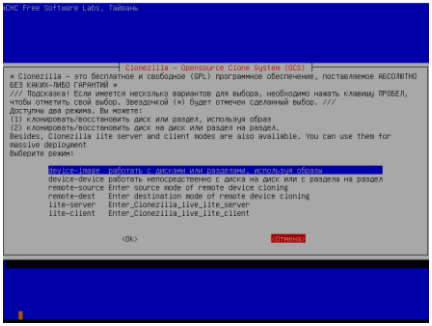

Рис. 1. Вибір у програмі *Clonezilla* режим роботи з дисками або розділами використовуючи образи

Після цього вибираємо команду rerun1 (рис. 2).

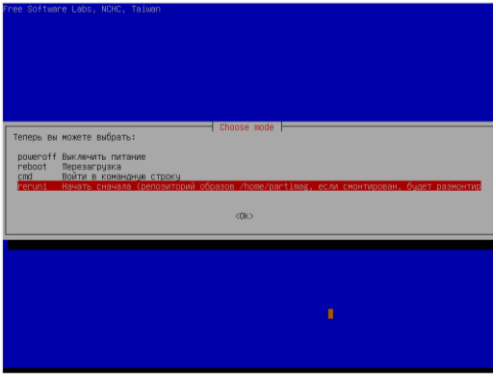

Рис. 2. Вибір команди команду rerun1

Для вибору необхідного диску на який буде встановлена резервна копія необхідно зі запропонованого списку вибрати створений попередньо резервний диск.

Зауваження. Щоб розрізняти новостворений розділ (резервний диск) необхідно задати йому мітку розділу, якщо цього не було зроблено раніше за допомогою програми GParted (п. 2). При цьому, перезапускаємо віртуальну машину і використовуючи програму GParted додаємо мітку розділу у новоствореному диску. Також розрізнити ці диски (зі встановленою ОС Debian та новостворений резервний диск)

можна порівнявши їх розміри, попередньо визначивши розмір диску зі встановленою ОС.

Після цього продовжуємо процес у Clonezilla з попереднього пункту. По завершенні створення резервної копії програма Clonezilla запропонує перевантажитися.

4. Перезавантажити віртуальну машину з ОС Debain. Після цього, затерти нулями завантажувальну область диска командою *sudo dd if=/dev/zero of=/dev/sda bs=1k count=1k* (якщо виконано вхід під користувачем *root*, то виконуємо команду без *sudo*).

Зауваження. Виконуючи попередню дію ми імітуємо пошкодження диску, або операційної системи.

5. Переконатись в неможливості завантаження ОС Debian з даного жорсткого диска, перезапустивши ОС. Завантаження не повинно відбуватися у зв'язку з тим, що ми пошкодили завантажувальну область (повинно з'явитися повідомлення про фатальну помилку).

6. Відновити встановлену ОС Debian з раніше створеної резервної копії за допомогою програми *Clonezilla*, повторно заватажившись з *Live CD Clonezilla* та обравши при розгортанні образу диска в якості цільового диска той, на якому був знищений завантажувальний запис. Переконатись в нормальному завантаженні відновленої ОС.

Для виконання цього процесу запускаємо знову Clonezilla так як в п. 3, проводимо ті ж самі налаштування, проте в кінці обираємо опцію *restoredisk*. Потрібно вказати *відновити образ з диску* вказавши шлях до папки в якій зберігається резервна копія та вибрати режим відновлення, як показано на рис. 3, при цьому має запуститися процес відновлення.

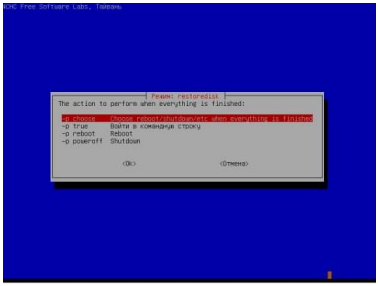

Рис. 3. Вибір режиму відновлення

6. Очікуємо результат копіювання резервної копії Після відновлення перезапускаємо віртуальну машину і переконуємося, що ОС Debian знову запускається у нормальному режимі.

7. Результати виконання оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму та порядок виконання роботи;
- скріншоти з описами виконання кожного пункту *Порядку виконання роботи.*
- скріншоти та описи: форматування диска в *ext4*, виконання команди *dd* та результату розгортання образу на диск;
- висновок.

Контрольні запитання

1. Назвіть приклади подій, після яких необхідно відновлення даних або всієї системи з резервної копії.
2. Які розрізняють рівні резервного копіювання?
3. Чи завжди можливо виконати повне резервне копіювання системи?
4. В чому різниця між LiveCD та LiveUSB?
5. Яким чином можна завантажити ОС на ПК, який не має можливості підключення зовнішніх носіїв даних?
6. Що таке образ диска та які вимоги ставляться до його зберігання?

Лабораторна робота №5
Безпека передачі даних при використанні протоколів TFTP, FTP, Telnet, SSH

Мета роботи

Ознайомитись з можливостями протоколів FTP, TFTP, Telnet та SSH та навчитись встановлювати та налаштовувати TFTP, FTP, Telnet, SSH-сервери та клієнти, а також розглянути способи забезпечення безпеки передачі даних при їх використанні.

Теоретичні відомості

Протокол передавання файлів *FTP* (File Transfer Protocol) — це протокол, який використовується для передавання файлів через Інтернет. Протокол FTP зазвичай застосовується для того, щоб зробити файли доступними для завантаження. З його допомогою можна завантажувати web-сторінки в процесі створення чи модернізації web-сайту, виконувати обмін зображеннями та ін.

Протокол передачі файлів *TFTP* (Trivial File Transfer Protocol) в основному використовується для первинного завантаження бездискових робочих станцій. На відміну від FTP протокол TFTP не містить можливостей аутентифікації (хоча можлива фільтрація за IP-адресою). Цей протокол заснований на транспортному протоколі UDP.

Telnet (англ. TErminaL NETwork) — мережевий протокол для реалізації текстового інтерфейсу через мережу. Часто вживається у вигляді програми-клієнта, тому Telnet — це програма з текстовим інтерфейсом, яка дає змогу підключитись до іншого комп'ютера через Інтернет за цим протоколом. Якщо власник або адміністратор надає право підключитися до ПК, то програма *Telnet* дає змогу вводити команди для доступу до програм і служб на віддаленому комп'ютері, ніби так, як би ви працювали безпосередньо за ним. Програму Telnet можна використовувати для доступу до електронної пошти, баз даних і файлів. Як правило, Завдяки простоті програмної реалізації Telnet часто використовується для доступу до вбудовуваних систем, або мережевого обладнання.

Оскільки у протоколі *Telnet* не передбачено використання ні шифрування, ні перевірки достовірності даних, то він вразливий

для будь якого виду атак, до яких вразливий протокол TCP. Тому для доступу до UNIX-подібних операційних систем використовується інший протокол - SSH.

SSH (англ. Secure SHell — «безпечна оболонка») — мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і здійснювати тунелювання TCP-з'єднань (наприклад, для передачі файлів). SSH схожий за функціональністю з протоколом *Telnet* і *rlogin*, проте шифрує весь потік даних, в тому числі, передані паролі.

Криптографічний захист протоколу SSH не фіксований, він надає вибір різних алгоритмів шифрування. Крім того, цей протокол дозволяє не тільки використовувати безпечний віддалений *shell* (командний інтерпретатор, який використовується в Unix сумісних операційних системах) на ПК, тобто виконувати команди, які подає користувач, або які читаються з файлів, але і тунелювати графічний інтерфейс — X Tunnelling (тільки для Unix-подібних ОС або програм, що використовують графічний інтерфейс X Window System). SSH здатний передавати через безпечний канал будь-який інший мережевий протокол (Port Forwarding), забезпечуючи можливість безпечної передачі не тільки X-інтерфейсу, але і, наприклад, звуку та відео.

Для роботи по протоколу SSH потрібен SSH-сервер і SSH-клієнт. SSH-сервер прослуховує з'єднання від клієнтських ПК і при встановленні зв'язку виконує аутентифікацію, після чого починає обслуговування клієнта. SSH-клієнт використовується для входу на віддалений ПК і виконання команд. Для з'єднання SSH-сервер і SSH-клієнт повинні створити пари відкритих і закритих ключів та обмінятися ними, при цьому також використовується пароль.

Програма роботи

1. Встановити FTP-сервер та перевірити можливість підключення до нього та передачу даних.
2. Встановити TFTP-сервер та перевірити можливість підключення до нього та передачу даних.
3. Встановити Telnet-сервер та перевірити можливість підключення до нього та передачу даних.

4. Встановити SSH-сервер та перевірити можливість підключення до нього та передачу даних.

Порядок виконання роботи

1. Переконатись, що при підключенні віртуальної машини встановлений тип підключення мережевого адаптера: *проміжний адаптер/мережевий міст*. Запустити ОС Debian у віртуальній машині, видалати *Dnsmasq* командою *sudo apt-get purge dnsmasq*. Занотувати IP-адресу віртуальної машини після виводу даних команди *sudo ip a*.

2. Виконати встановлення сервера *vsftpd* (Very Secure FTP Daemon). Для цього виконуємо команду *sudo apt-get install vsftpd*, а також встановити FTP-клієнт командою *apt install ftp*. Налаштувати сервер, відредагувавши файл конфігурації */etc/vsftpd.conf*. У цьому файлі знаходимо рядок *listen* замінюємо у ньому значення з *NO* на *YES.*

Для цього, подібно, як у попередній лабораторній роботі використовуємо файловий менеджер *MC* запуск якого здійснюється командою *sudo mc* (відповідно без *sudo*, якщо ви працюєте під користувачем *root*). Навігація по об'єктах у каталозі здійснюється клавішами керування курсором, перехід у батьківський каталог (на рівень вище) – вибором *.. (дві крапки)*, перегляд текстового файлу – натисканням *F3*, редагування – *F4* (рис. 1).

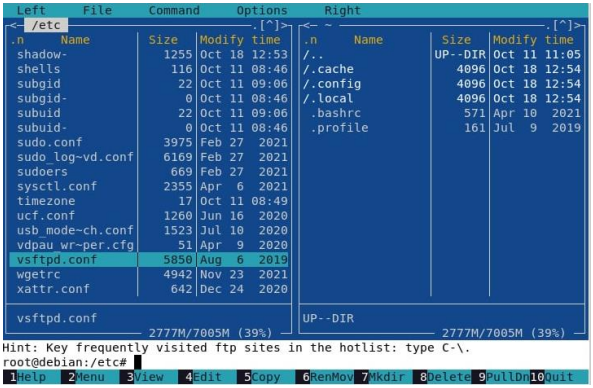

Рис. 1. Вигляд вмісту папки */etc/* з виділеним файлом *vsftpd.conf* у файловому менеджері *MC*

Для редагування файлу *vsftpd.conf* використовуємо текстовий редактор *Nano* (див. попередні лабораторні роботи) (рис. 2).

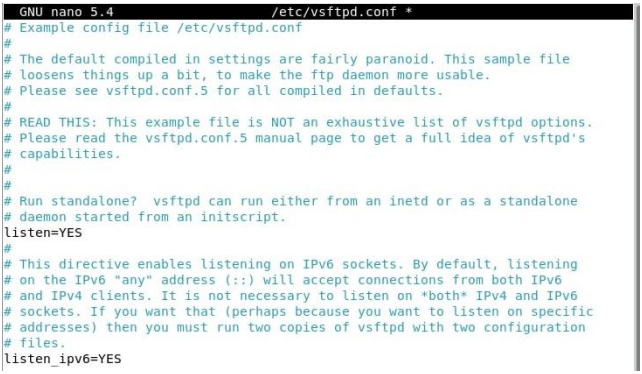

Рис. 2. Вміст файлу *vsftpd.conf* при його редагуванні текстовим редактором *Nano*

Після виконання змін перезапускаємо FTP-сервер командою *sudo service vsftpd restart* (відповідно без *sudo*, якщо ви працюєте під користувачем *root*).

3. Перевірити можливість логіну (входу) на сервер командою *ftp localhost*, ввівши логін та пароль користувача. У випадку, якщо логін і пароль *ftp*-користувача співпадає з логіном і паролем локального користувача (ОС Debian) вхід буде виконано без запиту пароля, у іншому випадку необхідно буде ввести логін і пароль, який, як правило, відповідає локальному (той самий що при вході в Debian). При успішному підключенні буде виведено запрошення вводу команд: *ftp>* (рис. 3).

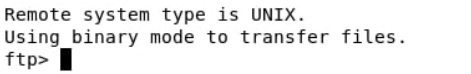

Рис. 3. Вигляд виконання команди при вході на *ftp*-сервер

3. Під’єднатись з хост-системи до віртуальної машини як до віддаленого хосту за допомогою FTP-клієнта (використавши IP-адресу гостьової системи) та створити у будь-якій папці новий текстовий файл на сервері. Скористаємося вбудованим FTP-

клієнтом ОС Windows. Для цього у вікні *Провідника* потрібно перейти в меню «*Комп'ютер*», а потім обрати ярлик: «*Підключити мережевий диск > Підключитися до веб-сайту, де можна зберігати документи та зображень»*. При цьому, використати IP-адресу збережену з п. 1, та виконати всю послідовність дій по підключенню (рис. 4).

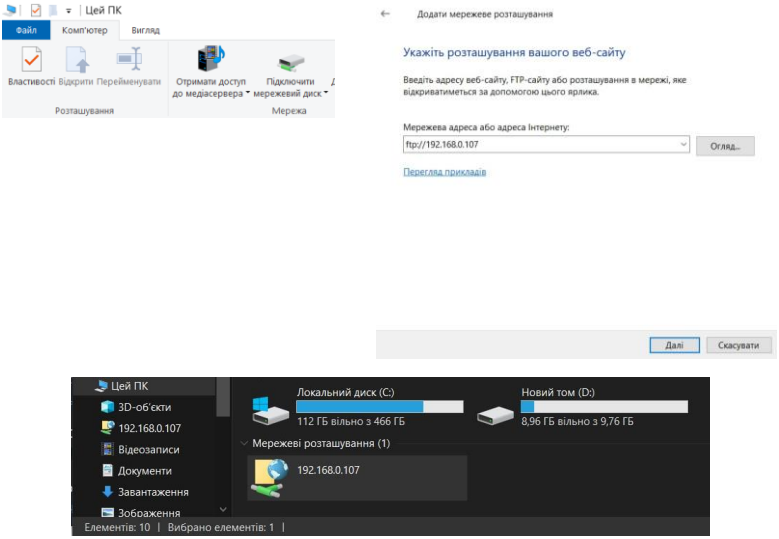

Рис. 4. Процес підключення хост-системи до віртуальної машини

Після цього потрібно повернутись до терміналу гостьової системи (в режимі віртуальної машини у ОС Debian) та вивести вміст зміненої теки командою *ls -la ~*. При цьому, отримаємо результат, який показано на рис. 5 та зберігаємо його у звіт.

```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la ~
output to local-file: /root?
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
local: /root: Is a directory
226 Directory send OK.
225 No transfer to ABOR.
ftp>
```

Рис. 5. Опис вмісту зміненої теки

5. Встановити TFTP-сервер TFTPD-HPA командою *sudo apt-get install tftpd-hpa*. Змінити налаштування сервера у файлі */etc/default/tftpd-hpa*, вказавши в якості шляху до кореневого каталога файлової системи для клієнтів каталог */srv/tftp* (може бути вказаний за замовченням) (рис. 6). Після цього скопіювати в цей каталог файл *timezone*. Це можна зробити використовуючи програму *MC*, тобто відкрити обидва каталоги у різних вікнах програми *MC* та виконати копіювання так, як показано на рис. 7.

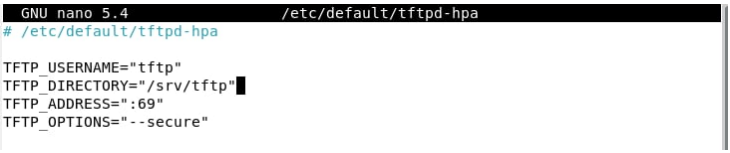

Рис. 6. Параметри налаштування сервера у файлі */etc/default/tftpd-hpa*

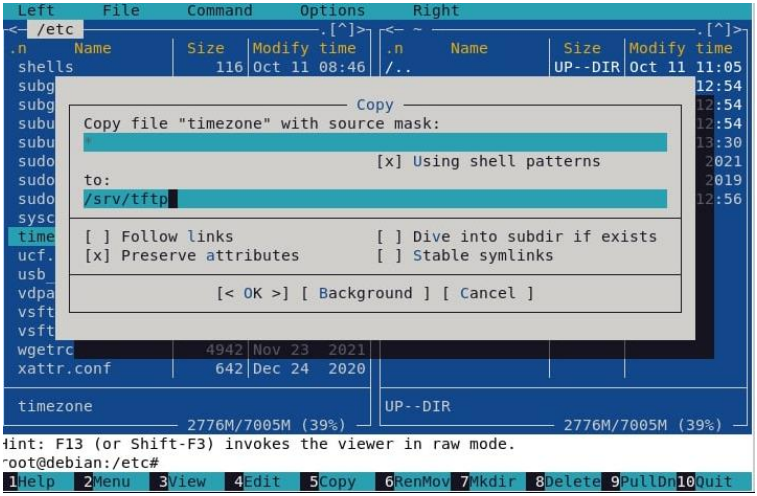

Рис. 7. Процес копіювання файлу *timezone* в каталог */srv/tftp*

Після цього, перезапустити TFTP-сервер використовуючи команду service *tftpd-hpa restart*. Під'єднатись до нього з хост-системи (ОС Debian) за допомогою безкоштовної програми TFTPD32, яку можна завантажити з сайту *https://bitbucket.org/phjounin/tftpd64/downloads/* та скопіювати

файл *timezone* на хост-систему так, як показано на рис. 8. При цьому, файл з вказаного сервера скопіюється на локальний комп'ютер у вказаний каталог. Таким чином, ми встановили TFTP-сервер та перевірили можливість підключення до нього та виконали передачу даних.

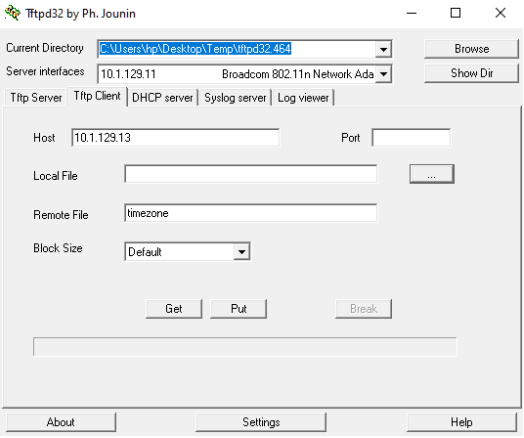

Рис. 8. Копіювання файлу *timezone* на хост-систему

6. Встановити *Telnet*-сервер виконавши команду: *sudo apt-get install telnetd*. Під'єднатись до гостьової системи за протоколом *Telnet* за допомогою програми *PuTTY* (*putty.exe (the SSH and Telnet client itself)*), яку можна запустити з сайту *https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html*. У вікні *PuTTY* виконати команду, наприклад *uname -a*. Зберегти результат у звіт та після виконання всіх дій відключитись від *Telnet*-сервера.

7. Підключитись до гостьової системи за допомогою SSH. Це можна зробити використовуючи ту ж саму програму *PuTTY* вказавши відповідний тип SSH (рис. 9).

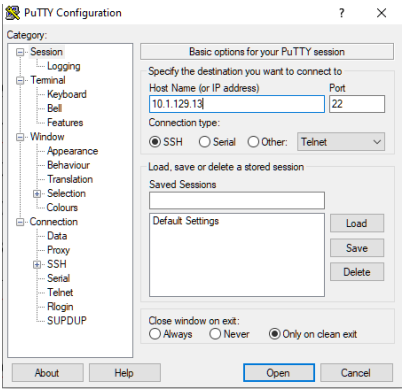

Рис. 9. Робота програми PuTTY в режимі SSH

Після цього отримаємо повідомлення з відображенням ключа для підключення до сервера, яке копіюємо у звіт (рис. 10). Застосування ключа дасть змогу перевірити, що підключення здійснюється справді до потрібного вузла, а не вузла зловмисника з іншим ключем.

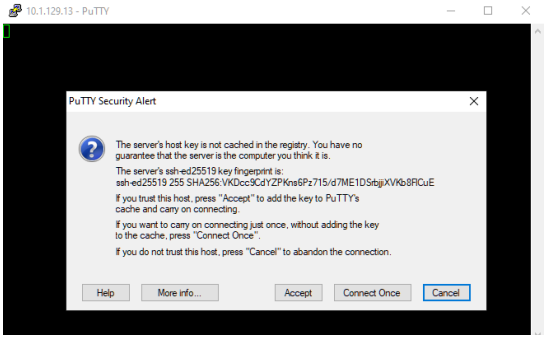

Рис. 10. Відображення ключа з програми PuTTY в режимі SSH

Зауваження. Якщо для входу буде використовуватися логін *root*, то потрібно дозволити його вхід з паролем змінивши у файлі */etc/sshd/sshd_config* рядок з налаштуванням *PermitRootLogin* на значення *yes* видаливши встановлений за замовчуванням параметр. Після цього перезавантажити SSH-сервер командою *service sshd restart*.

Після виконання з'єднання видаліть *TFTP*- та *Telnet*-сервери командою *sudo apt-get purge tftpd-hpa telnetd*.

8. Результати виконання команди з використанням протоколу SSH скопіюйте в звіт. Після завершення вказаних дій виконайте команду *sudo poweroff*.

9. Результати виконання всіх пунктів оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму роботи;
- скріншоти з пунктів порядку виконання роботи;
- скріншоти файлів усіх налаштувань;
- висновок.

Контрольні запитання

1. Яке призначення й особливості протоколу Telnet?
2. Яке призначення й особливості протоколу SSH?
3. Яке призначення й особливості протоколу FTP?
4. Яке призначення й особливості протоколу TFTP?
5. Як запустити FTP-клієнт у Windows?
6. Як перезапустити сервер VSFTPD?

Лабораторна робота №6
Тема: Захист даних безпроводових мереж

Мета роботи

Ознайомитись з будовою і призначенням основних складових безпроводової мережі Wi-Fi. Навчитися використовувати технології захисту безпроводовго Wi-Fi-з'єднання.

Теоретичні відомості

Технологія Wi-Fi (IEEE 802.11) - це сімейство технологій безпроводового передавання у радіодіапазоні. Сімейство стандартів IEEE 802.11 визначає фізичний та канальний рівень протоколів передавання, вони відрізняються фізичною реалізацією та швидкістю. Серед існуючих Wi-Fi мереж найпоширенішим є стандарт IEEE 802.11b, він дає змогу передавати дані зі швидкістю 11 Мбіт/с на відстань до декількох кілометрів, використовуючи смугу частот 2.4 Гц. На основі IEEE 802.11b будують безпроводові локальні мережі Wireless LAN (WLAN). Мережа Wi-Fi може працювати в двопунктових сполученнях, однак найчастіше використовують один або декілька пунктів доступу.

Принцип дії мережі Wi-Fi. Кожен Wi-Fi-адаптер (станція) постійно сканує ефір у пошуку сигналів від пунктів (точок) доступу. Сканування буває пасивним та активним. При пасивному скануванні Wi-Fi-адаптер переглядає окремі канали в пошуку найсильнішого сигналу з пунктів доступу. А кожен пункт доступу періодично передає сигнал (кадр) присутності. В цьому кадрі є ідентифікатор пункту та доступні швидкості передавання. При активному скануванні Wi-Fi-адаптер сам ініціює сканування, передаючи кадр вимоги на передавання, а пункти доступу відповідають кадрами присутності і надалі процес відбувається так, як при пасивному скануванні.

Після сканування відбувається процес автентифікації, який ініціює Wi-Fi-адаптер, що передає запит до пункту доступу. Цей пункт перевіряє запит і підтверджує або відхиляє його. Wi-Fi-адаптер після успішної автентифікації обирає пункт доступу, з яким буде працювати та узгоджує швидкість передавання. Пункт доступу відповідає кадром підтвердження у якому наводиться

додаткову інформацію про себе. Після цього, починається сеанс передавання.

Режими аутентифікації у Wi-Fi-мережах:

1. *Відкрита аутентифікація*. Підключення відбувається без пароля, шифрування не використовується, всі дані передаються у відкритому вигляді тому вони можуть бути перехоплені.

2. *Personal (персональна аутентифікація)*. Використовується єдиний пароль для всіх пристроїв у мережі, при цьому кількість пристроїв обмежена (невелика).

3. *Enterprise (відокремлена аутентифікація)*. Використовуються визначені паролі для різних користувачів з використанням сервера аутентифікації (застосування протоколів Radius, LDAP), захищеність користувачів найвища, але необхідно використовувати спеціальне обладнання.

Для розгортання Wi-Fi-мережі використовують безпроводові точки доступу і безпроводові адаптери. Однак у найпростішому випадку для передачі даних через Wi-Fi-з'єднання навіть не потрібно використання точки доступу. Серед режимів функціонування Wi-Fi-мереж широкого застосування отримали: *Infrastructure* і *Ad Hoc*.

У режимі *Ad Hoc*, що також називають *Independent Basic Service Set (IBSS)*, або *Peer to Peer* (точка-точка), вузли мережі безпосередньо взаємодіють один з одним без участі точки доступу. Цей режим потребує мінімального устаткування: кожен Wi-Fi-клієнт такої мережі повинен бути оснащений тільки Wi-Fi-адаптером. При такій конфігурації не потрібно створення мережної інфраструктури. Основними недоліками режиму Ad Hoc є: обмежений діапазон дії мережі і неможливість підключення до зовнішніх мереж. Якщо обидва Wi-Fi-клієнти перебувають у безпосередній близькості, або в межах прямої видимості, то режим Ad Hoc дозволяє об'єднати їх у одну мережу. Такий режим може бути ефективним при передачі даних з одного пристрою на інший. Але, якщо необхідно об'єднати в таку Wi-Fi-мережу пристрої розташовані на більших відстанях, або в різних приміщеннях, то режим Ad Hoc не ефективний, оскільки потужності передавачів і чутливості приймачів для забезпечення стійкого з'єднання буде недостатньо. У такому випадку для організації ефективної Wi-Fi-мережі потрібно застосовувати

стаціонарну точку доступу. Перевагою цього підходу є те, що це дає змогу розширити зону покриття (радіус дії) Wi-Fi-мережі.

Точка доступу в безпроводовій мережі виконує функцію, яка аналогічна до функції комутатора традиційної кабельної мережі і дозволяє поєднувати всіх клієнтів у єдину мережу. Завдання точки доступу - координувати обмін даними між всіма клієнтами мережі і забезпечити всім клієнтам рівноправний доступ до середовища передачі даних.

Режим функціонування безпроводової мережі на базі точки доступу називається - *Infrastructure Mode*. Розрізняють два різновиди режиму Infrastructure Mode: основний *BSS (Basic Service Set)* і розширений *ESS (Extended Service Set)*. У режимі BSS всі вузли мережі зв'язуються між собою тільки через одну точку доступу, що може виконувати також роль моста до зовнішньої мережі. А у розширеному режимі, тобто ESS, використовується інфраструктура з декількох мереж BSS, причому самі точки доступу взаємодіють одна з одною, що дозволяє передавати дані від однієї BSS до іншої. Між собою точки доступу з'єднуються за допомогою кабельної мережі, або радіомостами.

Стандарти безпроводового зв'язку. Існує кілька основних типів безпроводових стандартів: 802.11a, 802.11b і 802.11g та ін. Відповідно до цих стандартів використовуються різні типи устаткування:

- 802.11a – високошвидкісний стандарт WLAN для частоти 5 ГГц. Підтримує швидкість передачі даних 54 Мбіт/с;

- 802.11b – стандарт WLAN для частоти 2,4 ГГц. Підтримує швидкість передачі даних 11 Мбіт/с;

- 802.11g – встановлює додаткову техніку модуляції для частоти 2,4 ГГц. Призначений для забезпечення швидкостей передачі даних до 54 Мбіт/с.

Устаткування безпроводових мереж включає *точки доступу* (Access Point) і *безпроводові адаптери*. Точки доступу виконують роль концентраторів, що забезпечують зв'язок між абонентами та між собою, а також функцію мостів, що здійснюють зв'язок з кабельною локальною мережею та з Інтернетом. Декілька близько розташованих точок доступу утворюють зону доступу Wi-Fi, в межах якої всі абоненти, які мають безпроводові адаптерами

отримують доступ до мережі. Такі зони доступу (*Hotspot*) створюються в місцях масового скупчення людей: в аеропортах, студентських кампусах, бібліотеках, офісах, бізнес-центрах і т. п.

Метод доступу до мережі – CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) забезпечує можливість кожній точці доступу обслуговувати декількох абонентів, але чим більше абонентів до неї під'єднано, тим менш ефективна швидкість передачі для кожного з них. На українському ринку представлені точки доступу і безпроводові маршрутизатори компаній 3Com, Asus, Asante, D-Link, Gigabyte, MSI, Multico, Trendnet, US Robotics, ZyXEL, SMC та ін.

Налаштування точки доступу. Найкращий способом налаштування точки доступу за допомогою комп'ютера (зі встановленим мережним адаптером Ethernet), який підключений до мережевого комутатора. Розглянемо приклад налаштування точки доступу TP-Link TL-WR814N. Для цієї точки доступу за замовчуванням встановлена IP адреса 192.168.0.1 з маскою підмережі 255.255.255.0. Для того, щоб приступити до налаштування точки доступу необхідно призначити комп'ютеру статичну IP адресу з тієї ж підмережі, що і для TP-Link TL-WR814N. Для налаштувань параметрів TCP/IP протоколів потрібно перейти в меню: «*Панель керування → Мережа й Інтернет → Мережеві підключення*» і виконати налаштування в спеціальному мережевому інтерфейсі.

Для налаштування підключення точки доступу до мережі потрібно перейти у браузері за адресою 192.168.0.1 ввівши її в полі адресації. Також для даного типу роутера можна ввійти ввівши в полі адреси браузера http://tplinklogin.net. *Зауваження*. IP-адреса повинна бути в межах локальної мережі, тобто 192.168.0.X. У вікні авторизації необхідно ввести логін і пароль. За замовчуванням у багатьох точках доступу використовується логін: *admin* та пароль: *admin*, або порожнє поле. Для точного визначення цих параметрів необхідно звернутися до технічної документації на точку доступу. Після успішної авторизації відкривається сторінка з налаштуваннями точки доступу (рис. 1). Основні налаштування безпроводової мережі за допомогою меню виконують за допомогою меню *Мережа* (*Сеть*) приведено на рис. 2.

Технології захисту бездротових мереж. *WEP* (Wired Equivalent Privacy) — стандарт захисту, який ґрунтується на методі потокового кодування з використанням алгоритму RC4 (загальний секретний ключ). *WPA* (Wi-Fi Protected Access) - технологія захисту, яка грунтується на протоколі TKIP (Temporal Key Integrity Protocol), що використовує стійкий механізм шифрування. TKIP змінює ключ шифрування для кожного переданого пакета, що ускладнює можливість його підбору. *WPA PSK* (WPA Pre-Shared Key) – це спрощена версія технології WPA, яка може застосовуватися для невеликих безпроводових мереж. У ній, як і в WEP, використовується статичний ключ, але він автоматично змінюється в певних часових інтервалах. *WPA2* є покращеною версією WPA та більш захищеною завдяки заміні TKIP на CCMP (блочне шифрування з кодом автентичності повідомлень). На даний час застосування WPA2 є обов'язковою для всіх сертифікованих Wi-Fi пристроїв. *WPA2 PSK* – це спрощена версія WPA2, яка аналогічна до WPA PSK, але з використанням AES-шифрування.

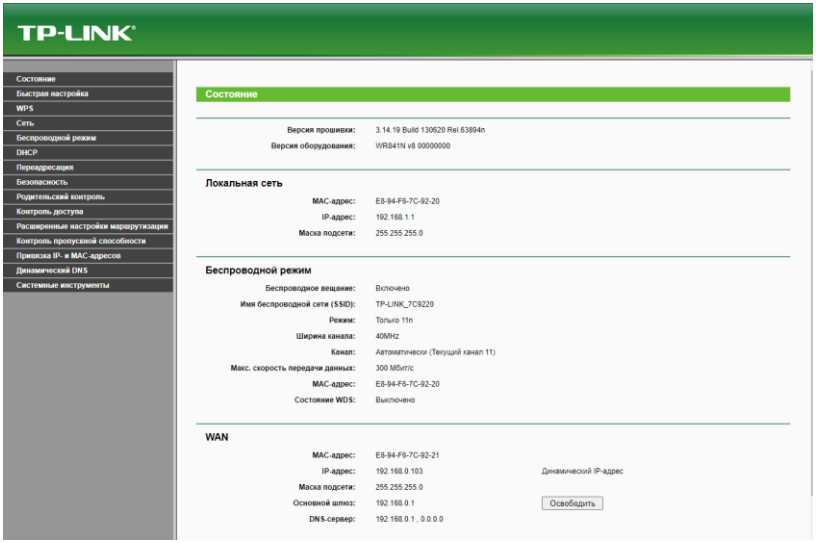

Рис. 1. Основне меню налаштуваннями TP-Link TL-WR814N

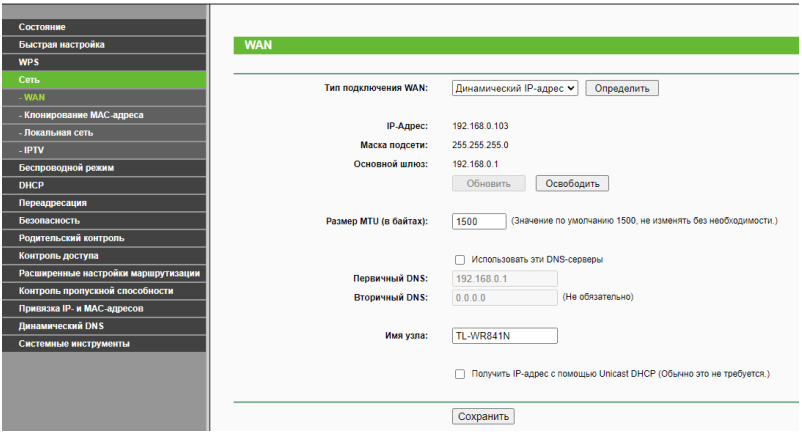

Рис. 2. Основні налаштування безпроводової мережі

Налаштування сервісу DHCP. DHCP – це протокол динамічної конфігурації, який дає змогу отримувати динамічні IP-адреси. На рис. 3 показано варіанти настроювання конфігурації DHCP. При ввімкнені DHCP пристрої можуть отримувати IP адресу автоматично з вказаного діапазону (*Начальній IP-адрес*). Така IP адреса буде змінюватися через певні проміжки вказаного часу (*Срок действия адреса*). Більшість сучасних мобільних пристроїв (смартфони, планшети) не мають налаштувань статичної IP-адреси, тому для їх нормального функціонування у цій мережі потрібно ввімкнення служби DHCP.

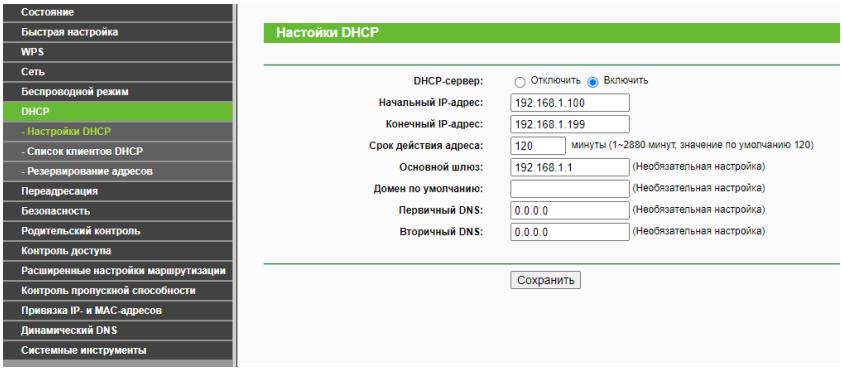

Рис. 3. Настроювання протокола динамічної конфігурації DHCP

Для перегляду різної статистичної інформації: списку підключених вузлів, помилок та інших параметрів використовується меню *Состояние* (рис. 4).

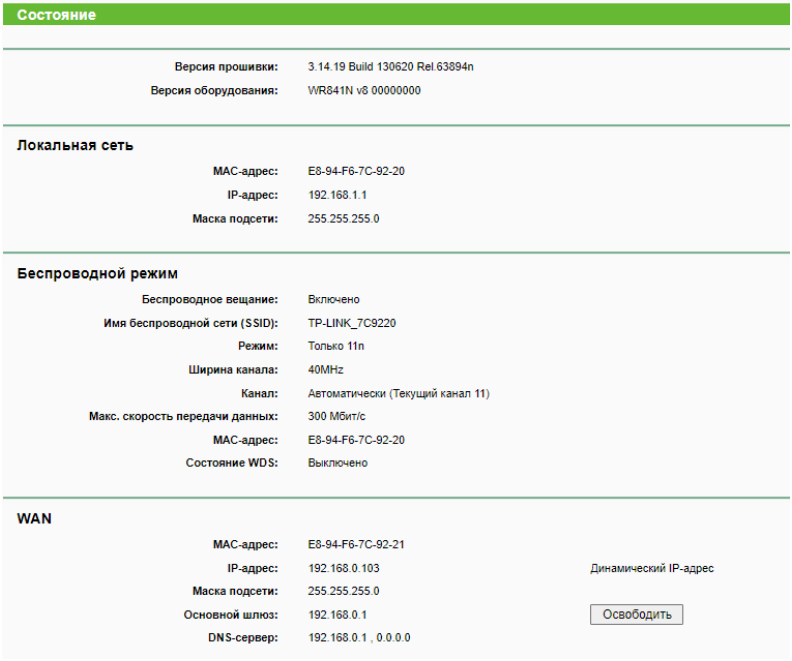

Рис. 4. Вигляд меню *Состояние*

Налаштування списку дозволених комп’ютерів за MAC-адресами можна виконати у додаткових налаштуваннях *Advanced* (рис. 5).

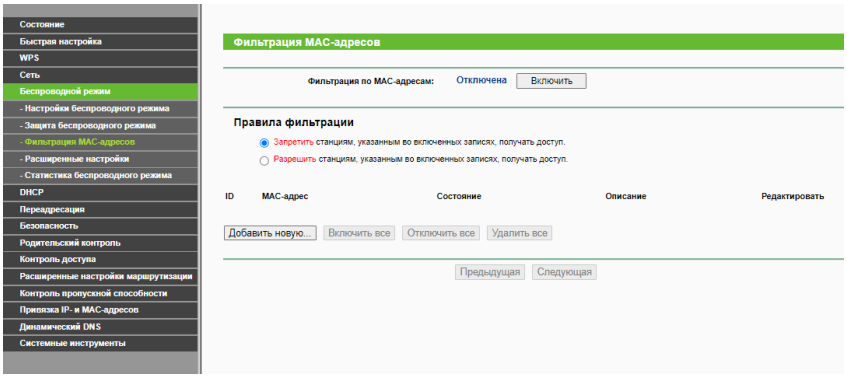

Рис. 5. Меню налаштувань параметрів MAC-адрес

Використовуючи *Tools*–меню для налаштувань прав доступу (рис. 6) можна обмежити доступу приховавши назву точки доступу. Це дасть змогу, приховати її видимість для інших, а при необхідності підключення до неї потрібно ввести її ім’я.

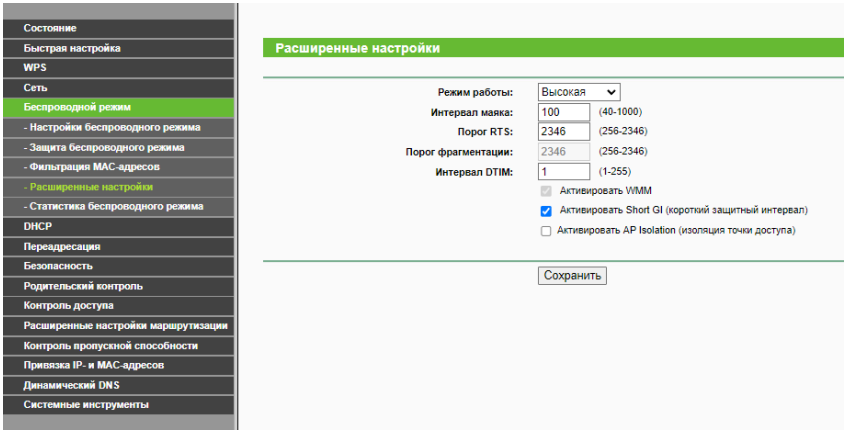

Рис. 6. Меню для додаткових налаштувань безпеки

Налаштування безпроводового Wi-Fi з’єднання на комп’ютері з ОС Windows. Для того щоб переглянути доступні безпроводові мережі і під’єднатися до Wi-Fi-мережі на локальному комп’ютері з операційною системою Windows 10 необхідно натиснути на відповідне зображення мережевого підключення у правому

нижньому куті рядку стану. Після цього з'явиться перелік доступних безпроводових мереж. Для того щоб переглянути властивості безпроводової мережі можна у цьому ж вікні поряд з кнопкою доступних мереж натиснути на вкладку «*Налаштування мережі та інтернету*», або перейти в меню: «*Панель керування → Мережа й Інтернет → Мережеві підключення → Стан Wi-Fi → Властивості безпроводової мережі*» (рис. 7).

Підключення до невидимої мережі. Щоб налаштувати підключення до невидимої мережі (тієї яка не надсилає повідомлення з SSID ідентифікатором) потрібно перейти в пункт «*Стан Wi-Fi → Властивості безпроводової мережі*» та на відповідній вкладці вибрати необхідну мережу і зазначити галочку «*Підключатися,навіть якщо мережа не передає своє ім'я (SSID)*» (рис. 7).

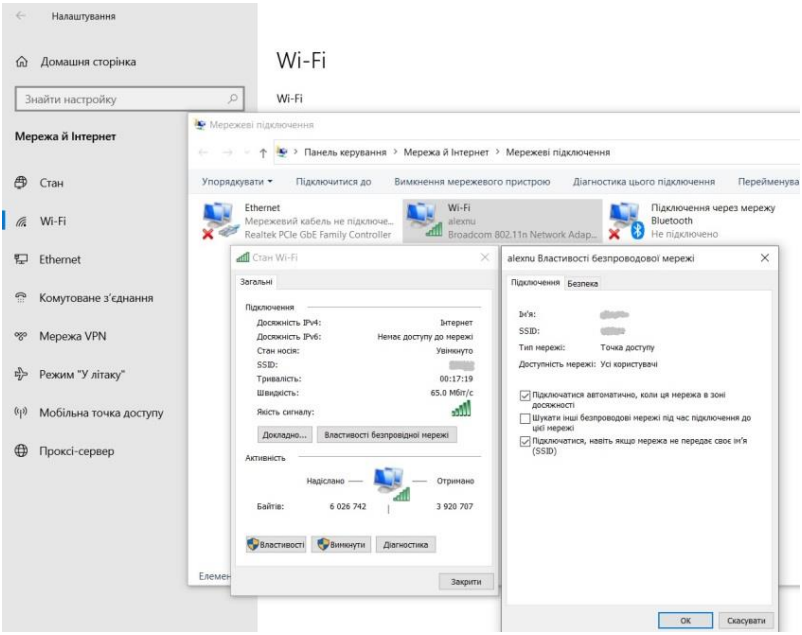

Рис. 7. Настроювання безпроводової мережі

Також можемо здійснити інші налаштування мережі та методи її аутентифікації.

Програма роботи

1. Ознайомитися з будовою і призначенням основних складових безпроводової мережі Wi-Fi.

2. Навчитися використовувати технології захисту безпроводовго Wi-Fi-з'єднання.

Порядок виконання роботи

1. Під'єднати точку доступу (Wi-Fi маршрутизатор) до локального комп'ютера за дпомогою патч-корда RJ45. *Зауваження*. У якості прикладу використано Wi-Fi маршрутизатор TP-Link TL-WR841N. У випадку використання іншого маршрутизатора опис меню з налаштуваннями можуть відрізнятися.

2. Налаштувати TCP/IP властивості для під'єднання до точки доступу та записати попередні налаштування. Для цього необхідно перейти: *Панель керування > Мережа й Інтернет > Мережеві підключення > Ethernet > Властивості Протокол інтернету версії 4 (TCP/IPv4) - властивості.*

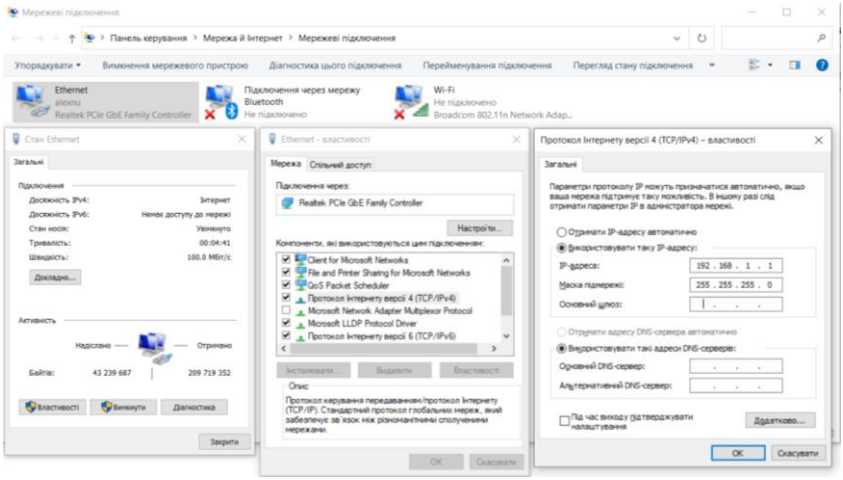

Рис. 8. Налаштування TCP/IP властивості для під'єднання до точки доступу

3. Перевірити зв'язок з точкою доступу за допомогою утиліти *ping* ввівши вказану IP-адресу (рис. 9).

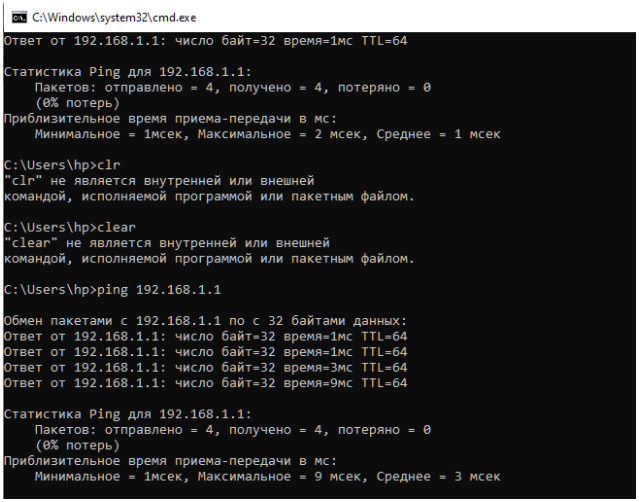

Рис. 9. Перевірити зв’язок з точкою доступу

4. Ознайомитись з наявними налаштуваннями маршрутизатора (меню *Status*):

- DHCP-сервера;
- MAC-адреси підключених пристроїв;
- алгоритм шифрування даних у безпровідній мережі;
- швидкість з’єднання;
- потужність сигналу та ін.

Щоб зайти в налаштування маршрутизатора необхідно в браузері відкрити сторінку за адресом основного шлюзу (див. п.2). У стандартних налаштуваннях часто використовують IPv4 (192.168.0.1), який береться з налаштувань TCP/IP протоколу. В різних маршрутизаторах він може відрізнятися, зазвичай він вказаний в документації до нього, або на самій точці доступу. Також для входу на цю сторінку потрібно мати логін і пароль адміністратора точки доступу, він також вказаний в документації, або на зворотній стороні маршрутизатора.

5. Використовуючи меню *Настройка беспроводного режима* (рис. 10). Після цього змінюємо назву точки доступу (SSID) на довільну.

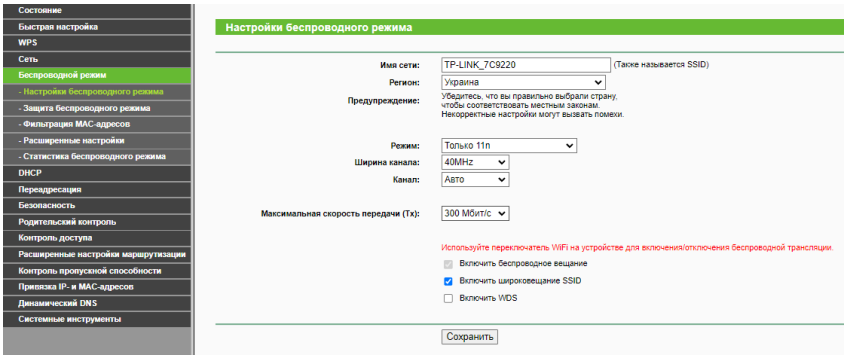

Рис. 10. Зовнішній вигляд меню маршрутизатора з вибором налаштування мережі

6. Змінюємо параметри налаштування мережі натиснувши (*редаг*.) ввівши назву мережі, у нашому прикладі це - ххх та режими роботи маршрутизатора, подібно як це показано на рис. 11.

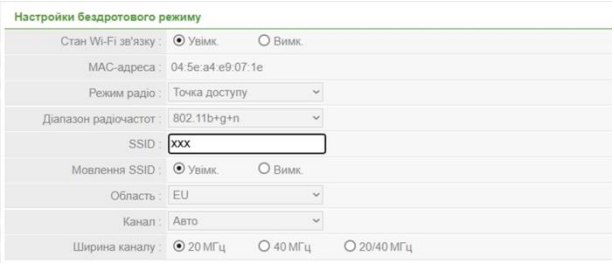

Рис. 11. Зміна назви точки доступу (SSID)

7. Вибираємо тип шифрування даних та задаємо пароль доступу (рис. 12).

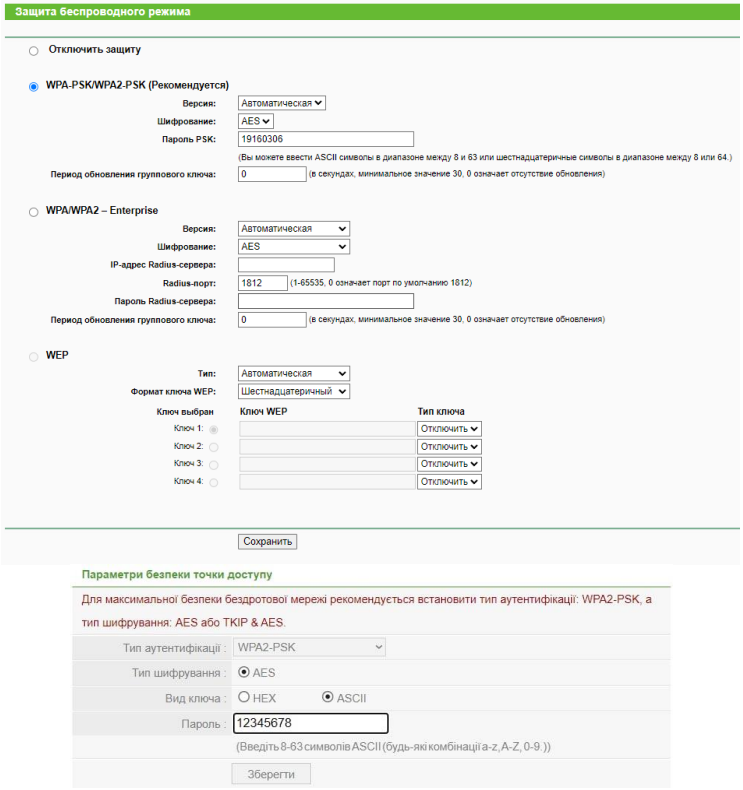

Рис. 12. Приклад зміни типу шифрування та пароля доступу для різних типів маршрутизаторів

8. Виконуємо підключення до налаштованої точки доступу та перевіряємо наявність з’єднання (рис. 13).

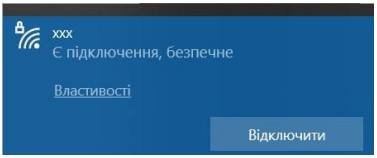

Рис. 13. Перевірка можливості з’єднання з маршрутизатором

9. Під’єднатися до точки доступу з довільного пристрою та провести тестування з’єднання за допомогою утиліт *ping*, *netstat*

та ін. (рис. 14).

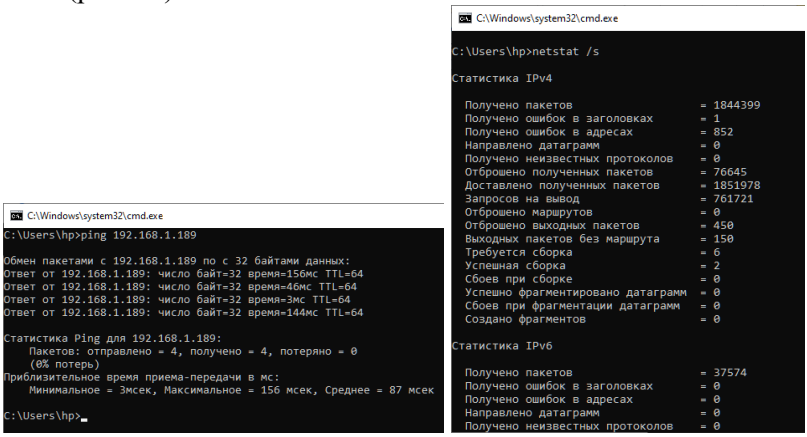

Рис. 14. Перевірка з’єднання з маршрутизатора за допомогою утиліт *ping*, *netstat*

10.Змінити параметри аутентифікації (WPA-PSK, WPA2-PSK та ін.) почергово перевіряючи та доналаштовуючи з’єднання на маршрутизаторі.

11.Знайти під’єднаний/ні пристрій/ої в меню статистики на точці доступу та зафіксувати їх MAC-адреси (у нижчеподаному прикладі доступні тільки 3-и пристрої) (рис. 15).

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
Redmi7A-Redmi	192.168.1.189	c8:3d:dc:14:33:1d	11h 56m 13s
?	192.168.1.227	40:2c:f4:02:5d:07	11h 33m 1s
Aleks	192.168.1.221	64:31:50:09:73:83	11h 46m 21s

Рис. 15. MAC-адреси під’єднаних пристроїв

12.Виконати тестування роботи фільтру MAC-адрес. Для цього спочатку заблокуйте доступ до тестованого пристрою вказавши його MAC-адресу, а потім дозвольте підключення тільки цьому пристрою (рис. 16).

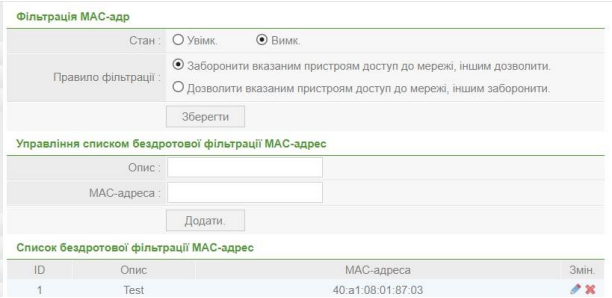

Рис. 16. Налаштування фільтрації за MAC-адресами

13.Виконати приховування точки доступу (SSID) за допомогою встановлення відповідної відмітки (рис. 17) та перевірити результат за допомогою стороннього пристрою.

Рис. 17. Виконання приховування маршрутизатора

14.За допомогою послідовності, яка описана в теоретичних відомостях та показана на рис. 7 виконати під'єднання до прихованої (невидимої) мережі та протестувати це з'єднання.

15.Записати параметри налаштувань точки доступу зробивши резервну копію (*load settings from local hard drive*). Цей пункт необхідно виконати кожного разу, коли ви вносите зміни в налаштування пристрою.

16.Від'єднати точку доступу від локального комп'ютера та повернути налаштування TCP/IP до початкових значень.

17.Провести та перевірити налаштування рівня безпеки використовуючи інший пристрій (роутер) та порівняти з описаним в теоретичних відомостях.

18.Виконати налаштування рівня безпеки власного домашнього роутера з тими ж пунктами, що і попередні два пристрої.

19.Проаналізувати та порівняти рівні безпеки досліджуваних трьох пристрої та описати їх вразливості.

20.Результати виконання всіх пунктів оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму роботи;
- скріншоти виконання всіх пунктів, які описані у порядку виконання роботи;
- описи процесу виконання з поясненнями виконаних дій;
- висновок.

Контрольні запитання

1. Що таке Wi-Fi?
2. Які стандарти Wi-Fi ви знаєте?
3. Яка максимальна швидкість Wi-Fi?
4. Яке обладнання використовується для безпроводового доступу?
5. Де і як здійснюється налаштування безпроводової точки доступу?
6. Які налаштування потрібно задати для підключення на локальному комп'ютері?
7. Що таке SSID?
8. Які стандарти шифрування ви знаєте?
9. Як приховати точку доступу?
10. Що таке DHCP, для чого він використовується?
11. Як дозволити підключення до точки доступу лише певним пристроям?
12. Як повернути налаштування точки доступу в початковий стан?

Лабораторна робота №7
Застосування системи виявлення вторгнень в комп'ютерну систему

Мета роботи

Ознайомитися з існуючими системами виявлення та запобігання вторгнень. Навчитись застосовувати та налаштовувати систему виявлення вторгнень OSSEC.

Теоретичні відомості

Система виявлення атак (вторгнень) — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними через Інтернет. Системи виявлення вторгнень (англ. Intrusion Detection System, IDS) забезпечують додатковий рівень захисту комп'ютерних систем разом з системою запобігання вторгненням (англ. Intrusion Prevention System, IPS).

IDS можуть сповістити про початок атаки на мережу, причому деякі з них здатні виявляти раніш не відомі атаки. IPS не обмежуються лише сповіщенням, але й здійснюють різні заходи, спрямовані на блокування атаки (наприклад, розрив з'єднання або виконання скрипта, який заданого адміністратором). На практиці досить часто програмно-апаратні рішення поєднують у функціональністъ двох типів систем, тоді їх називають IDPS (IDS і IPS).

Мережеві та системні IDS. Мережеві (Network-based IDS, NIDS) контролюють пакети в мережевому оточенні і виявляють спроби зловмисника проникнути всередину системи або реалізувати атаку «відмова в обслуговуванні». Ці IDS працюють з мережевими потоками даних. Типовий приклад NIDS — система, яка контролює велику кількість TPC-запитів на з'єднання (SYN) з багатьма портами на обраному комп'ютері, виявляючи, таким чином, що хтось намагається здійснити сканування TCP-портів. Мережева IDS може запускатися або на окремому комп'ютері, який контролює свій власний трафік, або на виділеному комп'ютері, прозоро «переглядає» весь потік даних у мережі (концентратор, маршрутизатор). Мережеві IDS

контролюють багато комп'ютерів, тоді як інші IDS контролюють тільки один. Прикладом мережевої IDS є система виявлення вторгнень запобігання атак - Snort, яка, комбінує методи зіставлення по сигнатурам, засоби інспекції мережевих протоколів і механізми для виявлення аномальних дій.

IDS, які встановлюються на хості і виявляють зловмисні дії на ньому, називаються хостовими або системними IDS. Прикладами хостових IDS можуть бути системи контролю цілісності файлів, які перевіряють системні файли з метою визначення, коли в них були внесені зміни. Системи моніторингу реєстраційних файлів (Log-file monitors, LFM), контролюють реєстраційні файли, створювані мережевими сервісами і службами. Прикладом хостової IDS є система OSSEC.

Статичні і динамічні IDS. Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе ПЗ, помилки в конфігураціях та ін. Статичні IDS перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів. Статичні IDS виявляють сліди вторгнення.

Динамічні IDS здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Динамічні IDS виконують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

Програма роботи

1. Ознайомитися з існуючими системами виявлення та запобігання вторгнень з теоретичних відомостей.
2. Встановити систему виявлення вторгень OSSEC, налаштувати та перевірити її роботу.

Порядок виконання роботи

1. Запутити віртуальну машину Oracle VM VirtualBox і у налаштуванні підключення до мережі вказуємо — *проміжний адаптер/мережевий міст*. Оновити індекс доступного в репозиторії програмного забезпечення командою *sudo apt-get*

update. Встановити наявні оновлення командою *sudo apt-get upgrade.*

Зауваження. Якщо вхід в ОС Debian здійснено під користувачем *root*, то команду *sudo* можна не застосвувати.

2. Встановити пакети, необхідні для роботи системи OSSEC: *sudo apt-get install build-essential apache2 libapache2-mod-php apache2-utils libpcre2-dev make zlib1g-dev libpcre2-dev libevent-dev libssl-dev libz-dev libsystemd-dev.* Встановити систему керування версіями *Git* командою *sudo apt-get install git.*

Зауваження. У деяких випадках для встановлення певних пакетів необхідно, у налаштуванні підключення до мережі віртуальної машини, перейти з *проміжний адаптер/мережевий міст* на *NAT*. Для повторного введення тих самих команд можна використовувати на клавіатурі стрілки ↑↓ верх/вниз.

3. Завантажити останні версії системи OSSEC та web-інтерфейсу до неї з Git-репозиторіїв за вказаними адресами https://github.com/ossec/ossec-hids, https://github.com/ossec/ossec-wui командою *git clone адреса_репозиторію.git*. Після цього встановлюємо оновлення командою *sudo ./install.sh.* Щоб виконати інсталяцію потрібно перейти у відповідний каталог *ossec-hids*, командою *cd.* Під час інсталяції краще вибирати англійську мову (*en*) та виконувати всі необхідні дії слідкуючи за процесом (як правило, відповідь на запит системи *y/n* необхідно вибирати *n*). Після виконання інсталяції запускаємо систему OSSEC командою *sudo /var/ossec/bin/ossec-control start* (рис. 1).

```
Cloning into 'ossec-wui'...
remote: Enumerating objects: 205, done.
remote: Total 205 (delta 0), reused 0 (delta 0), pack-reused 205
Receiving objects: 100% (205/205), 217.04 KiB | 1.94 MiB/s, done.
Resolving deltas: 100% (69/69), done.
root@debian:~# cd ossec-hids
root@debian:~/ossec-hids# ./install.sh
```

Рис. 1. Виконання інсталяції системи OSSEC та web-інтерфейсу до неї

4. Встановлюємо web-інтерфейс системи OSSEC. Для цього вміст каталогу *./ossec-wui* (необхідно попередньо знайти місце завантаження каталогу *./ossec-wui*) копіюємо в каталог */var/www*. Це можна зробити за допомогою програми *MC* (як в попередніх лабораторних роботах) (рис. 2).

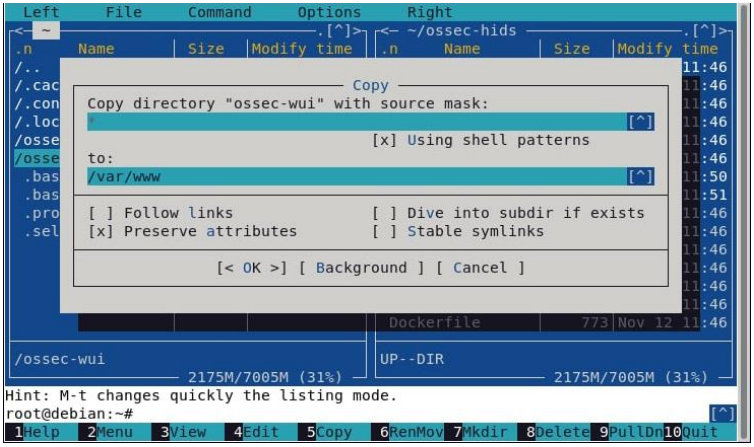

Рис. 2. Копіювання вмісту каталогу *./ossec-wui* в каталог */var/www*

Визначити каталог *./ossec-wui*, як кореневий каталог web-сервера. Для цього у файлі */etc/apache2/sites-enabled/000-default.conf* знайти рядок *DocumentRoot* і встановити властивість *DocumentRoot /var/www/ossec-wui,* зберегти зміни (рис. 3).

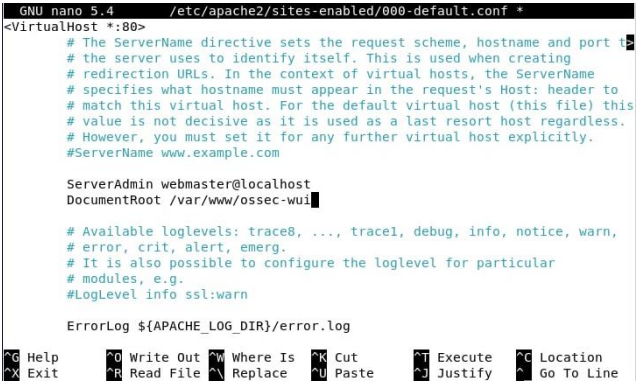

Рис. 3. Надання каталогу *./ossec-wui* властивостей кореневого каталогу web-сервера

Потім потрібно перейти у відповідний каталог *ossec-wui*,

командою *cd* і виконати команду *ossec-wui ./setup.sh.* Після цього ввести (створити) логін і пароль, вибрати ім'я сервера *www-data.*

5. Перезапустити web-сервер командою *sudo service apache2 restart* (Рис. 4) і відкрити сторінку у браузері http://IP-адреса_ПК_зі_встановленою_OSSEC/. При цьому, потрібно ввести IP-адресу віртуальної машини, яку можна перевірити по команді *IP a.*

```
bredemar@debian:~$ su -l
Password:
root@debian:~# service apache2 restart
root@debian:~#
```

Рис. 4. Перезапуск web-сервера

Після цього, за допомогою системи виявлення вторгнень ми зможемо проаналізувати всі події, які відбувалися з нашим сервером (рис. 5).

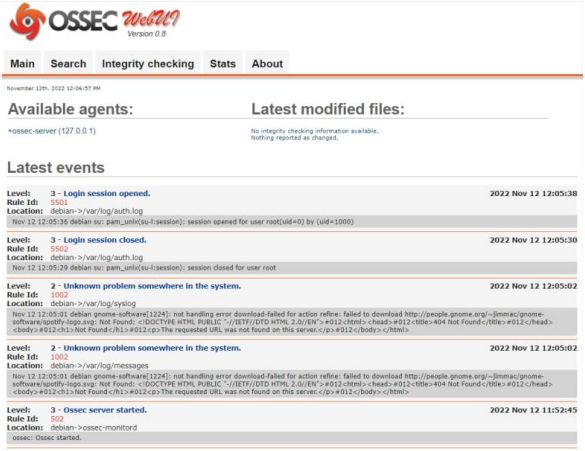

Рис. 5. Зовнішній вигляд системи OSSEC

6. Для перевірки дієвості системи виявлення вторгнень виконати сканування вузла (ПК) зі встановленою системою OSSEC за допомогою *Nmap* (рис. 6), занести в звіт результати.

Рис. 6. Сканування вузла (ПК) зі встановленою системою OSSEC за допомогою *Nmap*

7. Результати виконання всіх пунктів оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму роботи;
- скріншоти виконання всіх пунктів, які описані у порядку виконання роботи;
- описи процесу виконання з поясненнями виконаних дій;
- скріншоти виконання та результати сканування системи з OSSEC за допомогою Nmap;
- висновок.

Контрольні запитання

1. Що таке IDS?
2. Як класифікують IDS залежно від середовища аналізу?
3. Чим відрізняються динамічні IDS від статичних?
4. Для чого призначений log-file monitor?
5. Чим відрізняється IPS від IDS?

Лабораторна робота №8
Особливості захисту web-сайтів

Мета роботи

Навчитись використовувати елементи розробки та використання web-сайтів та організовувати їх захист

Теоретичні відомості

Web-сервер (англ. Web Server) — це сервер, що приймає HTTP-запити від клієнтів, зазвичай веб-браузерів, видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою, зображенням, файлом, медіа-потоком або іншими даними.

Також Web-сервером називають програмне забезпечення, що виконує функції web-сервера, так і комп'ютер, на якому це програмне забезпечення працює. У даній лабораторній роботі під терміном Web-сервер ми розумітимемо саме програмне забезпечення. Серед найбільш поширеного програмного забезпечення, яке виконує функції web-сервера є Apache HTTP-сервер.

Apache HTTP-сервер — це відкритий веб-сервер для UNIX-подібних, Microsoft Windows, Novell NetWare та інших операційних систем, який розробляється та підтримується спільнотою розробників відкритого програмного забезпечення під керівництвом Apache Software Foundation. Якщо користувач в рядку адреси браузера не вказав шлях до файлу, а лише адресу сайту, за замовчуванням web-сервер надсилає у відповідь файл *index.html*, *index.php* або інший, вказаний у налаштуваннях сервера. Каталог у файловій системі, у якому розміщений цей файл та інші файли і каталоги сайту, повинен бути визначений, як кореневий каталог web-сервера. Браузер користувача не може отримати доступ до файлів, які знаходяться за межами кореневого каталогу сервера (якщо у кореневому каталозі або у підкаталогах немає посилань за його межі).

Для динамічного створення HTML-сторінок у відповідь на запити користувача часто використовується мова PHP – інтерпретована мова програмування, код якої можна вбудовувати безпосередньо в *html-код* web-сторінок. Код PHP в HTML повинен знаходитись між початковим тегом *<?php* та

кінцевим *?>* (або між *<script language="php">* та *</script>*). Дані, необхідні для генерування web-сторінки-відповіді користувачеві, як правило, зберігаються в базах даних (БД). Одією з найпоширеніших систем управління базами даних (СУБД) є MySQL. *MySQL-сервер* виконує обробку SQL-запитів від інших програм, оновлення і керування реляційними БД, створення схеми бази даних і її модифікації, системи контролю за доступом до бази даних.

Система керування вмістом (англ. Content Management System, CMS) — це програмне забезпечення для організації web-сайтів чи інших інформаційних ресурсів в Інтернеті чи в окремих комп'ютерних мережах. Основні функції CMS: надання інструментів для створення вмісту web-сторінок, організація спільної роботи над вмістом, зберігання, контроль версій, дотримання режиму доступу, управління потоком документів, публікація вмісту, представлення інформації у вигляді, зручному для навігації, пошуку.

Велика частина сучасних систем управління вмістом реалізується у вигляді візуального *WYSIWYG редактора* – програми, яка створює html-код зі спеціальної спрощеної розмітки, що дозволяє користувачеві простіше додавати, редагувати й керувати вмістом сайту. Сайти, що використовують CMS, потребують для своєї роботи власне web-сервер, сховище даних (як правило, СУБД) і додаток, який власне реалізовує CMS (написаний на PHP, Perl або інших мовах програмування).

Однією з популярних CMS є *WordPress* — це проста у встановленні та використанні система керування вмістом з відкритим кодом. Сфера її застосування від блогів до складних web-сайтів. Вбудована система тем і плагінів в поєднанні з вдалою архітектурою дозволяє конструювати на основі WordPress практично будь-які web-проекти. Написана на мові програмування PHP з використанням бази даних MySQL. Оскільки WordPress є широковживаною системою, вона також є об'єктом кібератак. Тому при її використанні дуже важливо здійснювати захист web-сайтів.

Одним з популярних елементів захисту розроблених за допомогою WordPress сайтів є плагін (модуль) Wordfence. *Wordfence* здійснює сканування сайту на наявність вірусів,

шкідливих програм, троянських програм, шкідливих посилань і т.п. За допомогою Wordfence можна застосувати двоетапну авторизацію, заблокувати несанкціоновані спроби входу на сайт, додати у чорний список небажані IP-адреси або боти, які навантажують сервер, а також моніторити, з яких IP-адрес заходить в систему адміністратор сайту.

Програма роботи

1. Розглянути особливості використання різних елементів для розробки та використання web-сайтів з теоретичних відомостей.
2. Встановити web-сервер Apache, систему керування базами даних MySQL, інтерпретатор мови PHP, CMS Wordpress.
3. Навчитися використовувати можливості плагіну Wordfence виявляти несанкціоновані зміни структури web-сайтів.

Порядок виконання роботи

1. Запутити віртуальну машину Oracle VM VirtualBox, задавши тип підключення до мережі — *проміжний адаптер/мережевий міст*. Оновити індекс доступного в репозиторії програмного забезпечення командою *sudo apt-get update*. Встановити наявні оновлення командою *sudo apt-get upgrade*
2. Встановити найновіші компоненти, необхідні для роботи CMS Wordpress: web-сервер Apache, систему керування базами даних MySQL, інтерпретатор мови PHP, а також phpMyAdmin та MySQL-клієнт для адміністрування, командою *sudo apt-get install apache2 php7.4 php7.4-mysql mariadb-server mariadb-client.*

Зауваження. У даному прикладі вказано команди для інсталяції *php8.2 php8.2-mysql* з версією 8.2 (https://packages.debian.org/bookworm/php). Але якщо під час інсталяція ОС Debian повідомить про те, що версія вказаних продуктів застаріла, або не існує, то потрібно визначити найновіші, на даний час версії і встановити їх.

3. Завантажити CMS Wordpress командою *wget https://uk.wordpress.org/latest-uk.tar.gz.*
4. Розпакувати архів з CMS Wordpress командою *tar -xzvf latest-uk.tar.gz.*
5. За допомогою MySQL-клієнта під'єднатись до СУБД командою *mysql -u root -p* та виконати команди створення бази

даних з ім'ям *wordpressdb* і надання користувачеві *wordpressuser* з паролем *passwordforwp* всіх прав при роботі з усіма таблицями цієї БД. Виконати вихід з MySQL-клієнта командою *exit*.

6. Створити файл конфігурації системи керування вмістом. Для цього відкрити зразок файлу конфігурації командою *nano ./wordpress/wp-config-sample.php* та вказати дані, потрібні для доступу до бази даних. Замість фрагментів тексту *database_name_here, username_here, password_here* вписати вказані раніше ім'я бази даних логін та пароль так, як показано на рис 1. Зберегти змінений файл з ім'ям *wp-config.php* (Ctrl+O для збереження файлу, Y для підтвердження, Ctrl+X для виходу).

Рис. 1. Внесення змін у файл *wp-config-sample.php*

7. Перемістити каталог із сконфігурованою CMS у */var/www* командою *sudo cp -R ./wordpress /var/www* (рис. 2).

```
root@debian:~# nano ./wordpress/wp-config-sample.php
root@debian:~# nano ./wordpress/wp-config-sample.php
root@debian:~# sudo cp -R ./wordpress /var/www
root@debian:~#
```

Рис. 2. Виконання переміщення сконфігурованої CMS

8. У файлі налаштувань web-сервера Apache вказати в якості кореневого каталогу web-сервера шлях до каталогу */var/www/wordpress*: вікрити файл командою *sudo nano /etc/apache2/sites-enabled/000-default.conf* та замінити значення

властивості DocumentRoot на */var/www/wordpress.* Зберегти зміни (рис. 3).

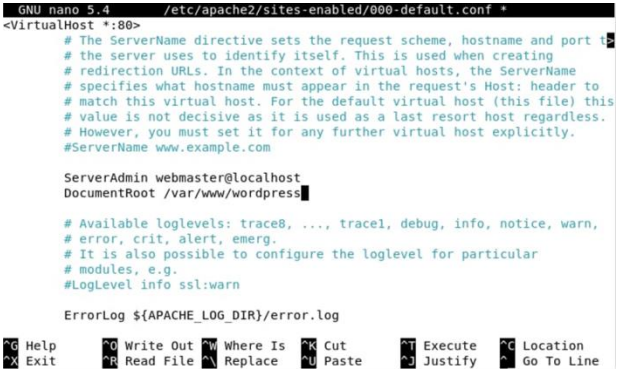

Рис. 3. Внесення змін у файл *000-default.conf*

9. Перезапустити web-сервер командою *sudo service apache2 restart.*

10. Ввести в рядок адреси web-браузера IP-адресу сервера (команда *ip a*), перейти на сторінку встановлення CMS Wordpress та виконати встановлення системи керування вмістом (ввести необхідну інформацію для створення сайту).

11. Після встановлення увійти з вашим логіном та паролем у адмін-панель CMS Wordpress, додати новий запис, останній рядок якого повинен містити ваше прізвище, та натиснути «Опублікувати». Відкрити знову головну сторінку сайту та переконатись, що запис опубліковано (web-сторінку створено).

12. Встановити плагін Wordfence. Для цього у адмін-панелі CMS Wordpress необхідно перейти в розділ плагіни і додати новий плагін Wordpress. Крім того, потрібно змінити налаштування встановленого раніше FTP-сервера вказавши в якості кореневого каталога */var/www/wordpress*, відредагувавши файл конфігурації */etc/vsftpd.conf*.

13. Перевірити можливості плагіну Wordfence виявляти несанкціоновані зміни структури. Для цього необхідно додати у файл *wp-login.php* за допомогою текстового редактора *nano* рядок *echo 'wordfence Test'* і запустити перевірку у браузері. Плагін Wordfence буде шукати всі відмінності файлів встановленого

WordPress від оригінальних і видасть інформацію про те, що відбулися несанкціоновані зміни.

14.Результати виконання всіх пунктів оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму роботи;
- скріншоти виконання всіх пунктів, які описані у порядку виконання роботи;
- описи процесу виконання з поясненнями виконаних дій;
- висновок.

Контрольні запитання

1. Що таке веб-сервер?
2. Які родини операційних систем підтримуються веб-сервером Apache?
3. Що таке PHP?
4. Як веб-сервер визначає, що в HTML-коді веб-сторінки є фрагмент PHP-коду, який потрібно передати для обробки PHP-інтерпретатору?
5. Що таке MySQL?
6. Які функції систем керування вмістом (контентом)?
7. Які програмні продукти необхідні для встановлення і роботи CMS Wordpress?
8. Що таке пагін Wordfence і як він працює?

Лабораторна робота №9
Аналіз та діагностика комп'ютерних мереж

Мета роботи

Навчитись використовувати засоби аналізу та діагностики комп'ютерних мереж для моніторингу та виявлення проблем при перегляді ARP-таблиць, передачі ехо-запитів, дослідженні шляху до вузлів, скануванні комп'ютерів у мережі.

Теоретичні відомості

ARP (англ. Address Resolution Protocol — протокол визначення адрес) — мережевий протокол, призначений для перетворення IP-адрес (адрес мережевого рівня) в MAC-адреси (адреси канального рівня) в мережах TCP/IP. Він визначений в стандарті RFC 826.

Перетворення адрес виконується шляхом їх пошуку за спеціальною таблицею. Ця таблиця називається ARP-таблицею, зберігається у пам'яті і містить рядки для кожного вузла мережі. В двох стовпчиках містяться IP- та Ethernet-адреси. Якщо потрібно перетворити IP-адресу в Ethernet-адресу, то відбувається пошук запису з відповідною IP-адресою. У ході звичайної роботи мережева програма відправляє прикладне повідомлення, користуючись транспортними послугами TCP. Модуль TCP посилає відповідне транспортне повідомлення через модуль IP. В результаті, складається IP-пакет, який має бути переданий драйверу Ethernet. IP-адреса місця призначення відома прикладній програмі, модулю TCP та IP. Необхідно на її основі знайти Ethernet-адресу місця призначення. Для пошуку відповідної Ethernet-адреси використовується ARP-таблиця.

ping — службова комп'ютерна програма (утиліта), призначена для перевірки з'єднань в мережах на основі TCP/IP. Вона відправляє запити (англ. Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді (англ. Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

Повна відсутність ICMP-відповідей може також означати, що

віддалений вузол (або якийсь із проміжних маршрутизаторів) блокує ICMP Echo-Reply або ігнорує ICMP Echo-Request.

Утиліта *ping* є одним з основних діагностичних засобів у мережах TCP/IP і входить у поставку всіх сучасних мережевих операційних систем. Функціональність утиліти *ping* також реалізована в деяких вбудованих операційних системах маршрутизаторів, доступ до результатів виконання *ping* для таких пристроїв за протоколом SNMP визначається відповідними стандартами.

Для отримання шляху проходження пакетів до певного вузла мережі використовують утиліту *tracert/traceroute*. Це службова комп'ютерна програма, яка призначена для визначення маршрутів прямування даних в мережах TCP/IP. *Traceroute* може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери з встановленою операційною системою Windows використовують ICMP-протокол, операційні системи Linux і маршрутизатори Cisco – протокол UDP. Приклад виконання програми для пошуку шляху до сервера з сайтом НУВГП наведений нижче:

>> tracert nuwm.edu.ua

Tracing route to nuwm.edu.ua [109.87.215.51]

over a maximum of 30 hops:

1 1 ms 1 ms 1 ms FV1 [192.168.2.1]

2 10 ms 1 ms 2 ms ip-37-221-140-1.airbites.net.ua [37.221.140.1]

3 1 ms 2 ms 2 ms c76-rv-dot1q-330.airbites.net.ua [188.230.88.5]

4 6 ms 7 ms 7 ms vl1526.c76-kv-g50.valor.ua [188.230.88.242]

5 6 ms 7 ms 7 ms vl1523.c76-kv-l9.valor.ua [188.230.118.185]

6 7 ms 6 ms 6 ms mirohost-2-ix.giganet.ua [185.1.62.9]

7 15 ms 14 ms 15 ms uck-rivne.ett.ua [78.154.162.38]

*8 * * * Request timed out.*

9 14 ms 13 ms 15 ms nuwm.rv.ua [109.87.215.51]

Для сканування цілих мереж найчастіше використовується утиліта *nmap* (Network Mapper) – це безкоштовне відкрите

програмне забезпечення для дослідження та аудиту безпеки мереж і виявлення активних мережевих сервісів. З часу публікації в 1997 р. такий аудит став стандартом в галузі інформаційної безпеки. *Nmap* використовує багато різних методів сканування, таких як UDP, TCP (connect), TCP SYN (напіввідкрите), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN- NULL-сканування. *Nmap* також підтримує великий набір додаткових можливостей, а саме:

- визначення операційної системи віддаленого хоста з використанням відбитків стека TCP/IP;
- «невидиме» сканування;
- динамічне обчислення часу затримки і повтор передачі пакетів;
- паралельне сканування;
- визначення неактивних хостів методом паралельного ping-опитування;
- сканування з використанням помилкових хостів;
- визначення наявності пакетних фільтрів;
- пряме (без використання portmapper) RPC-сканування;
- сканування з використанням IP-фрагментації;
- довільне вказання IP-адрес і номерів портів сканованих мереж;
- можливість написання довільних сценаріїв (скриптів) на мові програмування Lua.

Синтаксис застосування утиліти *Namp*:

-sL – створює список працюючих вузлів без сканування портів;

-sP – перевіряє доступність вузла за допомогою ping;

-PN – зчитує всі доступні хости навіть якщо вони не відповідають на ping;

-sS/sT/sA/sW/sM – TCP сканування;

-sU – UDP сканування;

-sN/sF/sX – TCP NULL і FIN сканування;

-p – для вказівки діапазону портів для перевірки;

-sV – детальне дослідження портів для для визначення версій використаних служб;

-O – визначає операційну систему;

-T[0-5] – швидкість сканування;

-D – маскує сканування за допомогою фіктивних IP;

-S – змінює свою IP адресу на вказану;
-spoof-mac – визначити свою MAC адресу.

Програма роботи

1. Розглянути особливості використання засобів аналізу та діагностики комп'ютерних мереж для моніторингу та виявлення їх проблем з теоретичних відомостей

2. Отримати ARP-таблицю хост-системи та віртуальної машини.

3. Надіслати ехо-запит та визначити маршрут передачі даних до вузла з хост-системи та віртуальної машини в режимах проміжного адаптера і NAT.

4. Встановити утиліту Nmap та просканувати локальну мережу.

Порядок виконання роботи

1. Запутити віртуальну машину Oracle VM VirtualBox. Оновити індекс доступного в репозиторії програмного забезпечення командою *sudo apt-get update*. Встановити наявні оновлення командою *sudo apt-get upgrade.*

2. Переглянути ARP-таблицю системи командою *sudo arp -a*. Записати результати виводу команди у звіт.

3. Перевірити час передачі пакетів до вузлів мережі, наприклад en.wikipedia.org, або іннші за допомогою утиліти ping: *ping en.wikipedia.org, google.com* та інші. Перевірити час передачі пакетів до вузла вказавши його IP-адресу. Для зупинки виконання команди *ping* використати комбінацію CTRL+C. Виконати команду *ping* в ОС Windows та порівняти дані з її виконанням в ОС Debian.

4. Отримати маршрут до використаних вузлів командою tracert: *sudo traceroute.*

Перевірити параметри команди *tracert* у Windows:

-d - без дозволів у назвах вузлів.

-h максЧисло максимальне число стрибків при пошуку вузла.

-j списокВузлів - вибір маршруту по списку вузлів (тільки для IPv4).

-w таймаут - таймаут кожної відповіді в мілісекундах.

-*R* - трасування шляху (тільки IPv6).

-*S адресаДжерела* - використовувана адреса джерела (тільки IPv6).

5. Встановити пакет *nmap*: *sudo apt-get install nmap.*

6. Виконати сканування будь-якого вузла мережі за допомогою утиліти *Nmap* (приклад введення команди: *nmap -sn 192.168.1.1/24*), а також перевірити застосування синтаксису цієї утиліти, що приведений у теоретичних відомостях. Занести результати сканування у звіт.

7. Виконати вищевказані пункти задавши тип підключення до мережі віртуальної машини Oracle VM VirtualBox — *проміжний адаптер/мережевий міст* та *NAT* і порівняти їх значення.

8. Результати виконання всіх пунктів оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму роботи;
- скріншоти виконання всіх пунктів, які описані у порядку виконання роботи;
- описи процесу виконання з поясненнями виконаних дій;
- висновок.

Контрольні запитання

1. Для чого призначений ARP?
2. Яку інформацію надає програма *ping*?
3. Який результат роботи програми *tracert/traceroute*?
4. Що таке Nmap?
5. Якими можливостями володіє Nmap?