# **Модуль 1**

## **Знайомство з ІТ-безпекою**

### **Вступ до курсу**

Перш ніж перейти до наступного курсу, я хочу вас щиро привітати. Ви пройшли непростий шлях до завершального курсу цієї програми. Так, це було нелегко, але погляньте, якого прогресу ви досягли. Ви вивчили всі основи ІТ. Зараз ми на останньому курсі, який доповнить ваші базові знання. Ми поговоримо про безпеку. Без неї всі процеси, які ви вивчили до цього часу, можуть зазнати невдачі, а цього не хоче жоден ІТ-фахівець.

Перш ніж ми перейдемо до справи, ще раз представлюся. Ми зустрічалися ще на першому курсі, коли говорили про історію Інтернету й Інтернет речей. Мене звати Джіан Спікузза, і я керівник програм у відділі безпеки Android. Я допомагаю захищати понад 2 млрд пристроїв Android, випускаючи нові функції безпеки та керуючи ними для кожної версії Android (які мають назви десертів).

Скільки я себе пам’ятаю, я завжди любив техніку. Я працюю у сфері ІТ з 16 років, і на дозвіллі я любив читати книжки про нові технології й збирати сервери зі старих комп’ютерних деталей у підвалі батьківського будинку. Я ніколи не складав тести дуже добре, і доказом тому були мої оцінки. Але це не зупинило мене на шляху до успішної кар’єри. Я працював єдиним ІТ-спеціалістом на три некомерційні організації, поки здобував освіту. Це був ще той стрес – відповідати за все: від налаштування й адміністрування баз даних до навчання нових працівників роботі з електронною поштою та внутрішніми інструментами.

Озираючись назад, я розумію, що цей досвід був безцінним. І, звісно, важливою частиною моєї роботи у сфері ІТ була саме безпека. Тепер я працюю безпосередньо з виробниками обладнання, розробниками додатків і командами інженерів у Google, забезпечуючи найвищий рівень захисту для наших користувачів. Для багатьох із них мобільний телефон – це єдиний спосіб зв’язку з Інтернетом. І я відчуваю велике задоволення, знаючи, що моя робота суттєво впливає на людей в усьому світі, які так покладаються на свої пристрої. Щоб досягти успіху в кібербезпеці, іноді потрібно подумки поставити себе на місце нападника й завжди бути на крок попереду. Отже, ви готові робити добро, думаючи про погане? Тоді поїхали!

Цей модуль буде повністю присвячений питанням безпеки: як безпеку намагаються порушити та як ми захищаємося від цих атак. Наприкінці цього модуля ви зможете визначати й розпізнавати ризики, вразливості й загрози безпеці. Ви також зможете визначити найпоширеніші атаки на системи безпеки. Нарешті, ви зрозумієте, як безпека обертається навколо принципу КЦД, і що таке принцип КЦД.

Коли йдеться про безпеку, що найперше спадає вам на думку? Мабуть, це фізична безпека, щось на кшталт захисту майна від потенційних злодіїв, зачинення вхідних дверей уночі та зберігання цінних речей у безпечному місці. Але в сучасному цифровому світі гроші зберігаються не лише в гаманці. Кошти також зберігаються на банківських рахунках онлайн, до яких можна отримати доступ, знаючи пароль. Дехто з нас узагалі не носить із собою кредитних карток, а якщо й носить, то не в гаманці. Вони зберігаються на наших улюблених вебсайтах, щоб зручніше робити покупки.

Але ми турбуємося не лише через гроші. Більша частина нашого особистого світу зберігається на мобільних телефонах. SMS-повідомлення, фотографії, особисті дані, дані для входу в додатки й багато іншого – усе це зберігається всередині пристроїв, які ми носимо в кишенях. На жаль, ми живемо у світі, у якому деякі люди й організації намагаються викрасти дані в компаній, урядів і навіть простих людей, як ми з вами. Однак фільми дають спотворене уявлення про цих цифрових злодіїв. Вони не такі гламурні чи професійні, як вам може здаватися. Цифрові злодії не мають команди хакерів, не носять темні худі й не друкують несамовито на своїх терміналах цілими днями, сподіваючись зламати системи багатомільярдних компаній. Я не кажу, що такого не трапляється, – нам усім відомі такі випадки. Але зазвичай середньостатистичний інтернет-зловмисник має такий самий вигляд, як ми з вами, – це звичайна людина, яка випадково дізналася про діру у вашій системі безпеки, а потім нею скористалася.

Наприклад, злодій міг просто дізнатися, що ваш пароль – це кличка вашої собаки. Коли єдине, що захищає ваш банківський рахунок, – це слово Fido, у вас проблеми. Але так само, як фізичні пристрої сигналізації стримують потенційних грабіжників, існує також чимало способів запобігти порушенню нашої цифрової безпеки. У цьому курсі ви глибше зрозумієте комп’ютерну безпеку. Ви дізнаєтеся, як запобігти найчастішим комп’ютерним атакам. Ви зрозумієте різні протоколи й механізми безпеки, які використовуються на наших комп’ютерах, в Інтернеті та в наших мережах. Ви також більше дізнаєтеся про криптографію, автентифікацію й механізми доступу, що є важливими навичками для фахівця з ІТ-підтримки. Наприкінці курсу ми дамо вам необхідні інструменти для оцінки безпеки в організації та визначення оптимальних запобіжних заходів для її захисту.

Сьогодні майже кожна компанія або галузь значною мірою покладається на технології для ведення повсякденного бізнесу. Чи можете ви уявити собі компанію (велику чи малу), яка б працювала без електронної пошти, функціональних комп’ютерів чи Інтернету? Візьмімо, наприклад, маленьку компанію. Їй потрібні певні технології для доступу до кредитних карток. Нещодавні атаки, як-от крипточерв’як WannaCry і масштабні атаки з використанням бот-мережі Mirai, унаочнюють обсяг і масштаб того, як безпека впливає на всіх нас. До цього питання слід ставитися серйозно. Через нашу широку залежність від технологій цифрова безпека важливіша, ніж будь-коли раніше, і її вплив лише зростатиме в усіх галузях і аспектах нашого життя. Тож зробімо так, щоб ви були озброєні належними інструментами для захисту себе й своїх майбутніх клієнтів.

## **Шкідливе програмне забеспечення**

### **Тріада CIA**

Протягом усього цього курсу ми часто вживатимемо одну ключову абревіатуру – "КЦД" (англ. – CIA). Ні, я говорю не про Центральне розвідувальне управління США (теж CIA), хоча воно багато робить для національної безпеки. У нашому випадку "КЦД" означає "конфіденційність, цілісність і доступність". Ці три ключові принципи є основою того, що зазвичай називають "тріадою КЦД". Це керівна модель для розробки правил інформаційної безпеки. Ці три принципи допоможуть вам розробити правила безпеки на робочому місці та у ваших особистих середовищах.

Почнімо з конфіденційності. Конфіденційність означає зберігання в таємниці. В IT це означає зберігання наявних даних надійно прихованими від сторонніх очей. Один із методів конфіденційності, який ви напевно використовуєте щодня, – це захист паролем. Лише ви і ще, можливо, ваш партнер маєте знати пароль для доступу до банківського рахунку онлайн. Для забезпечення конфіденційності потрібно обмежити доступ до даних. Знати, як отримати доступ, мають лише ті, кому це абсолютно необхідно.

Літера "Ц" в абревіатурі "КЦД" означає цілісність. Цілісність – це збереження даних точними й неспотвореними. Дані, які ми надсилаємо чи отримуємо, мають залишатися незмінними протягом усього процесу. Уявіть, що ви завантажили файл з Інтернету. На вебсайті, з якого ви його завантажили, указано, що розмір файлу – 3 МБ. Але після завантаження виявилось, що справжній розмір файлу – 30 МБ. Це сигнал про небезпеку. Щось сталося під час завантаження, щось потенційно небезпечне. Можливо, на вашому жорсткому диску тепер існує небажаний файл. Як ви дізнаєтеся на наступних уроках, таке трапляється дуже часто.

І останнє, але не менш важливе. Літера "Д" у "КЦД" означає "доступність". Доступність означає, що наявна інформація легко доступна тим користувачам, яким вона необхідна. Це може означати багато речей, зокрема готовність до втрати даних або збою системи. Хакерські атаки мають на меті вкрасти у вас чимало речей: час, матеріальні цінності, вашу гідність. Іноді у вас крадуть час, який ви мусите витрачати на відновлення роботи сервісів. Деякі зловмисники утримують вашу систему в заручниках, доки ви не заплатите викуп. Звучить страшно, і насправді так і є. Але саме тому ви тут – щоб дізнатися, як не допускати подібних атак.

Протягом цього курсу ви дізнаєтесь, як кожний аспект безпеки пов’язаний із цими трьома ключовими принципами: конфіденційністю, цілісністю та доступністю.

### **Основні умови безпеки**

Перш ніж докладно розглянути, як зупиняти цифрових злодіїв,  прояснімо деякі терміни. Ми будемо використовувати ці терміни протягом усього курсу, тож їх слід добре зрозуміти.

Перший термін – "ризик". Це – можливість зазнати збитків у разі атаки на систему. Скажімо, ви купуєте новий телефон. Один із заходів безпеки для захисту вашого пристрою – налаштувати блокування екрана за допомогою пароля або ключа, щоб запобігти доступу інших осіб до ваших даних. Блокування екрана – це функція безпеки, що допомагає запобігти небажаному доступу шляхом створення дії, яку потрібно виконати, щоб увійти. Якщо ви вирішите не блокувати екран телефона, ви піддаєте себе ризику того, що хтось може легко отримати до нього доступ і викрасти ваші дані. Навіть просте додавання пароля чи блокування екрана може допомогти захистити ваші особисті дані або дані компанії від потрапляння до сторонніх осіб.

Наступний термін – "вразливість". Це недолік у системі, який можна використати, щоб її зламати. Вразливостями можуть бути прогалини, про які ви можете знати чи ні. Ви можете їхати в тривалу відпустку й зачинити всі двері та вікна у своєму будинку перед виходом. Але ви забудете зачинити вікно ванної кімнати. Тепер це вікно ванної кімнати – вразливість, яку грабіжники можуть використати, щоб проникнути у ваш будинок. Інший приклад: скажімо, ви створюєте додаток і активували обліковий запис для тестування під час розробки, але забули вимкнути його перед запуском додатка. Тепер у вашому додатку є вразливість, яку потенційно може виявити зловмисник. Є особливий тип вразливості, що називається "вразливість нульового дня". Це вразливість, яка не відома розробнику або постачальнику програмного забезпечення, але відома зловмиснику. Назва означає кількість часу, яку мав постачальник програмного забезпечення, щоб зреагувати й усунути вразливість, а саме "нуль днів".

Ще один ключовий термін – "експлойт". Це програма, за допомогою якої використовується вада безпеки чи вразливість. Зловмисники створюють експлойти для вразливостей, які знаходять у ПЗ, щоб заподіяти шкоду системі. Скажімо, зловмисниця виявляє вразливість нульового дня. Вона вирішує скористатися раніше не відомою вадою та пише код експлойту нульового дня. Цей код буде спрямований на використання цієї конкретної невідомої вади, щоб отримати доступ до систем і заподіяти їм шкоду. Не надто приємна новина.

Наступний важливий термін – "загроза". Це ймовірність небезпеки, яка може використати вразливість. Загрози – це просто можливі зловмисники, свого роду грабіжники. Не всі грабіжники намагатимуться проникнути у вашу оселю, щоб викрасти найцінніші речі, але вони можуть це зробити, а тому вважаються загрозами.

Наступний термін – "хакер". У світі безпеки це той, хто намагається проникнути в систему чи використати її. Більшість із нас асоціює термін "хакер" зі зловмисниками. Але насправді є два поширені типи хакерів. Є так звані "чорні хакери", які намагаються проникнути в системи, щоб зробити щось шкідливе. Але є й "білі хакери", які намагаються знайти слабкі місця в системі, але при цьому попереджають власників цих систем, щоб вони могли виправити ситуацію, перш ніж хтось інший заподіє шкоду. Існують й інші типи хакерів, але ці два – основні й найважливіші для нас зараз.

Останній термін, який потрібно знати, – "атака". Це – фактична спроба заподіяти шкоду системі. Дуже важливо усвідомлювати можливі загрози й вразливості системи, щоб мати змогу краще підготуватися до атак. Сумна реальність полягає в тому, що атаки на вашу систему будуть завжди. Але перш ніж почати пошук підземного сховища, щоб провести там решту своїх днів, подумайте про те, що існують способи виявляти та пом’якшувати атаки, і ми допоможемо вам навчитися це робити. У цьому модулі ми поговоримо про деякі найпоширеніші типи атак, які траплятимуться вам вдома й на роботі.

На цьому курсі ви дізнаєтеся, як убезпечити свої системи від цих атак. Виявляється, існують сотні способів атакувати вашу систему. Але також існують і сотні способів запобігти їм. Ми розглядатимемо не всі, а лише найважливіші з них. Тож відкиньте ідею з бункером і приготуйтеся до нових знань, бо ми говоритимемо про реальні речі – реальну безпеку.

### **Шкідливе програмне забезпечення**

Зловмисні програми – це різновид шкідливого ПЗ, що може використовуватися для отримання конфіденційної інформації, видалення чи змінення файлів. Зазвичай вони можуть використовуватися для будь-яких небажаних цілей. Найпоширеніші зловмисні програми, з якими ви будете стикатися, – це віруси, черв’яки, рекламне ПЗ, шпигунське ПЗ, трояни, руткіти, бекдори, ботнети… О так, я знаю, це довгий список. Але ми детально розглянемо кожен із них і навіть дізнаємося про деякі реальні випадки. Та наразі поговорімо про найпоширеніші форми шкідливих програм.

Віруси – це найвідоміший вид шкідливих програм. Вони працюють так само, як віруси у вашому організмі. Якщо ви захворіли, вірус прикріплюється до здорової клітини в організмі, а тоді відтворює себе й поширюється на інші здорові клітини організму. І раптом ви починаєте чхати, хрипіти й почуваєтеся жахливо. Комп’ютерний вірус прикріплюється до певного виконуваного коду, наприклад до програми. У роботі програми бере участь багато файлів, кожен із яких тепер вразливий до зараження вірусом. Отже, вірус реплікує себе в цих файлах, робить свою зловмисну справу та повторює це знову й знову, доки максимально не пошириться. Страшно, чи не так? Тримайтеся, ми лише розпочинаємо.

Черв’яки схожі на віруси, але їм не потрібно кудись прикріплюватися, щоб поширюватися. Черв’яки можуть жити самостійно й поширюватися через такі канали, як мережа. Відомим прикладом комп’ютерного черв’яка був ILOVEYOU (або "Love Bug"), який поширився на мільйони комп’ютерів з ОС Windows. Цей черв’як поширювався електронною поштою. Від когось надходив електронний лист із темою "I Love You" і вкладенням, яке насправді було черв’яком, замаскованим під текстовий файл листа кохання. Текстовий файл насправді був виконуваним файлом, який після його відкриття вчиняв багато атак, зокрема копіював себе в кілька файлів і каталогів, запускав шкідливі програми, заміняв файли, а після цього приховував себе. Черв’як поширювався, викрадаючи електронні адреси, що зберігалися на комп’ютері та в клієнтах чатів жертви. Потім він надсилав цей електронний лист усім контактам в адресній книзі. Love Bug поширився по всьому світу й спричинив збитки на мільярди доларів. Таке от кохання. Це лише одна з багатьох причин, чому в жодному разі не слід відкривати невідомі вкладення електронної пошти.

Рекламні програми – одна з найпомітніших форм зловмисних програм, з якими ви зіткнетеся. Більшість із нас бачить їх щодня. Рекламні програми – це програми, які показують рекламу й збирають дані. Іноді ми завантажуємо рекламні програми на законних підставах. Це стається, коли ви приймаєте умови обслуговування, які дозволяють використовувати безкоштовне ПЗ в обмін на показ реклами. Але в решті випадків вони можуть встановлюватися без вашої згоди та можуть робити шкідливіші речі, ніж просто показувати рекламу.

У грецькій міфології є відомий міф про вторгнення в місто Троя. Греки, які довго намагалися потрапити всередину міських стін, нарешті вирішили сховатися у велетенській дерев’яній статуї коня, яку начебто хотіли принести в дарунок. Троянці пропустили подарунок усередину, а тоді під покровом ночі греки вибралися зі статуї й напали на місто. У сфері комп’ютерної безпеки є зловмисні програми, що функціонують як троянський кінь і мають відповідну назву. Троян – це зловмисна програма, що маскується під щось одне, але робить зовсім інше. Точно як історичний троянський кінь, якого пустили в місто жителі Трої. Комп’ютерний троян має бути прийнятий користувачем, тобто користувач має запустити програму. Ніхто б не став із власної волі встановлювати зловмисну програму на комп’ютері, тому трояни спокушають вас установити їх, маскуючись під інші програми.

Шпигунські програми – це різновид зловмисних програм, які шпигують за вами. Вони можуть стежити за екраном вашого комп’ютера, натисканням клавіш, вебкамерами, а потім передавати чи транслювати всю цю інформацію іншій особі. Це не дуже добре. Клавіатурні шпигуни – поширений тип шпигунських програм, що записують кожне натискання вами клавіші. Така програма може фіксувати всі повідомлення, які ви набираєте, вашу конфіденційну інформацію, паролі й навіть більше.

Вимагачі – тип атаки, що утримує ваші дані або систему в заручниках, доки ви не заплатите певний викуп. Пам’ятаєте про принцип доступності, про який ми говорили в першому відео? Ця атака схожа на спосіб зменшити доступність нашої безпеки? Бінго! Саме так і є. Одним із нещодавніх випадків була атака вимагача WannaCry у травні 2017 року. Ця зловмисна програма, скориставшись вразливістю в старих системах Windows, заразила сотні тисяч комп’ютерів по всьому світу. Найбільш примітним стало те, що ця атака вимкнула системи Національних служб охорони здоров’я Англії, що викликало кризу в цій сфері. Атака вимагача WannaCry зруйнувала системи по всьому світу. Ці типи атак стають дедалі поширенішими, і нам треба бути готовими боротися з ними. Тому продовжуймо роботу.

### **Зловмисне програмне забезпечення. Продовження**

Продовжимо говорити про зловмисні програми.  Ми вже розглянули деякі з основних типів зловмисних програм, що зустрічаються в системі. Це, зокрема, зловмисні програми, віруси, черв’яки, рекламні та шпигунські програми й вимагачі. А якщо наші зловмисники могли б викрадати не лише, наприклад, дані, але й ресурси наших комп’ютерів, як-от процесора? Не хочу вас засмучувати, але й таке теж трапляється.

Існують шкідливі програми, які можуть використовувати чужий комп’ютер для виконання завдання, яке централізовано контролює зловмисник. Такі зламані комп’ютери називають "ботами". Мережу з одного або кількох пристроїв-ботів називають "ботнетом". Ботнети призначені для використання потужності комп’ютерів, під’єднаних до Інтернету, для виконання певної розподіленої функції. Візьмімо, наприклад, майнінг біткоїнів. Для майнінгу біткоїнів потрібен комп’ютер, ресурси якого використовуються для виконання певних обчислень. Наприкінці ви можете отримати винагороду у вигляді певної суми біткоїнів. Популярною атакою є створення ботнетів, щоб, зокрема, майнити біткоїни. Так, замість того, щоб виконувати обчислення на одному комп’ютері, зловмисники можуть мати їх тисячу, щоб виконувати обчислення й отримувати ще більше біткоїнів.

Бекдор – це спосіб потрапити в систему, якщо інші способи не дозволені. Це потаємний вхід для зловмисників. Бекдори найчастіше встановлюються після того, як зловмисник отримує доступ до вашої системи й хоче його зберегти. Навіть якщо ви виявили, що вашу систему зламано, ви можете не усвідомлювати, що в ній існує бекдор. Якщо так, вам потрібно заблокувати його, перш ніж він заподіє ще більшої шкоди.

Ще однією формою зломисних програм, яка може спричиняти чимало проблем, є руткіт. З назви "руткіт" випливає, що це набір для кореневого елемента, тобто набір програм чи інструментів, які може використовувати адміністратор. Він дозволяє змінювати рівень адміністратора операційної системи. Руткіт може бути важко виявити, оскільки він може приховуватися від системи за допомогою самої системи. Хитрий маленький паразит. Руткіт може запускати багато шкідливих процесів, але водночас ці процеси не видно в диспетчері завдань, адже руткіт може приховувати свою присутність.

Логічна бомба – це різновид шкідливих програм, що навмисно встановлюється. Після настання певної події або часу вона запускає зловмисну програму. Широковідомий випадок логічної бомби мав місце у 2006 році. Тоді один нещасливий системний адміністратор банку запустив логічну бомбу й вивів із ладу сервіси компанії, намагаючись знизити ціни на її акції. Колишнього співробітника спіймали й звинуватили в шахрайстві, а потім засудили до восьми років ув’язнення. Не найлогічніша логічна бомба.

<https://www.independent.co.uk/news/business/news/disgruntled-worker-tried-to-cripple-ubs-in-protest-over-32-000-bonus-481515.html>

## **Мережеві атаки**

### **Мережеві атаки**

Мережевою атакою, концепція якої досить проста, але яка може завдати великої шкоди, є атака DNS Cache Poisoning. Ви, мабуть, пам’ятаєте з курсу про основи комп’ютерних мереж, що DNS працює, отримуючи інформацію про IP-адреси й імена, щоб полегшити вам пошук сайту. Атака DNS Cache Poisoning обманним шляхом змушує DNS-сервер прийняти підроблений запис DNS, який указує на зламаний DNS-сервер. Після цього він повідомляє вам підроблені DNS-адреси, коли ви намагаєтеся отримати доступ до дійсних сайтів. Мало того, DNS Cache Poisoning може поширитися й на інші мережі. Якщо інші DNS-сервери отримують свою інформацію DNS від зламаного сервера, вони надаватимуть такі несправжні записи DNS іншим вузлам.

Кілька років тому в Бразилії сталася масштабна атака DNS Cache Poisoning. З’ясувалося, що зловмисникам удалось "отруїти" DNS-кеш кількох місцевих інтернет-провайдерів, вставляючи підроблені записи DNS для різних популярних сайтів, як-от Google, Gmail або Hotmail. Коли хтось намагався відвідати один із цих сайтів, він отримував підроблений запис DNS і спрямовувався на сервер, який контролював зловмисник, де розміщувався невеликий Java-аплет. Після цього користувача обманом змушували встановити аплет, що насправді був зловмисним банківським трояном для викрадення банківських облікових даних. Це приклад реальної шкоди, яку можуть заподіяти атаки DNS Cache Poisoning. Докладніше про це можна прочитати в наступній додатковій статті.

Атака "людина посередині" – це атака, у якій зловмисник розташовується між двома вузлами, які вважають, що спілкуються безпосередньо один з одним. Вочевидь, цю назву потрібно було б змінити, бо хакерами бувають не лише люди. Ця атака відстежує інформацію, що надходить на ці вузли та з них, і потенційно може змінювати її під час передавання.

Поширений вид атаки "людина посередині" – перехоплення сеансу або файлів cookie. Скажімо, ви увійшли в обліковий запис на сайт й забули вийти. Ви вже автентифікували себе на сайті та створили маркер сеансу, який надає вам доступ до цього сайту. Якщо хтось у цей час здійснював перехоплення сеансу, він може викрасти цей маркер і видати себе за вас на сайті, чого ви, звісно, не хотіли б. Це ще один привід подумати про принципи безпеки "КЦД". Ви завжди хочете бути впевнені в тому, що дані, які ви надсилаєте чи отримуєте, є цілісними й неушкодженими.

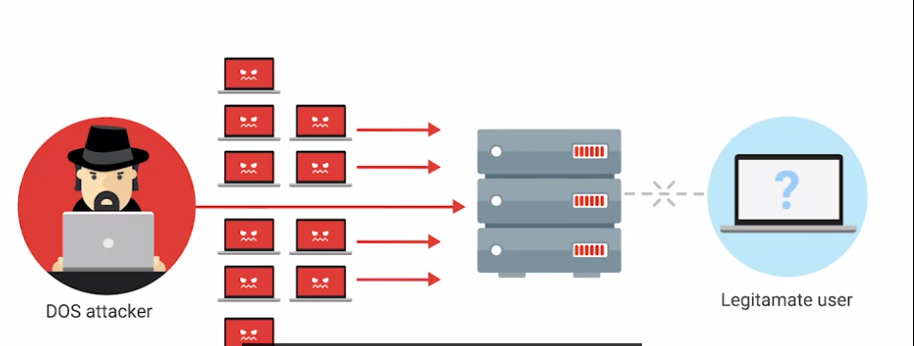
Ще один можливий спосіб атаки "людина посередині" – це атака з фальшивою точкою доступу. Фальшивою є точка доступу, установлена в мережі без відома її адміністратора. Іноді в корпоративних середовищах хтось може під’єднувати маршрутизатор до корпоративної мережі, щоб створити просту бездротову мережу. Звучить досить невинно, так? Насправді – ні! Це може бути досить небезпечно й може надати несанкціонований доступ до авторизованої захищеної мережі. Тепер зловмиснику, щоб отримати доступ до мережі, не потрібно підключатися безпосередньо до мережевого порту, а достатньо, просто стоячи за межами будівлі, під’єднатися до цієї бездротової мережі.

Останній спосіб атаки "людина посередині" називається "злий двійник". Вона схожа на фальшиву точку доступу, але має невелику, утім важливу відмінність. Атака "злий двійник" стає можливою, коли ви під’єднуєтеся до мережі, яка ідентична вашій. Ця ідентична мережа є "злим двійником" нашої мережі, і її контролює зловмисник. Щойно ми під’єднаємося до неї, він зможе відстежувати наш трафік. Цікаво: Фред Візлі коли-небудь робив таке з Джорджем? Мабуть, ні – вони ж чарівники. Вони б вирішували свої проблеми за допомогою магії. Мабуть, це круто.

<https://threatpost.com/major-dns-cache-poisoning-attack-hits-brazilian-isps-110711/75859/>

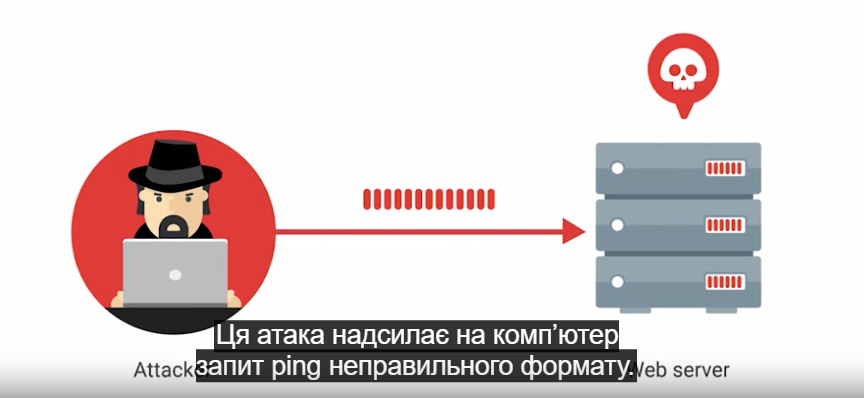
### **Відмова в обслуговуванні**

Атака "відмова в обслуговуванні" (DoS) – це атака, що намагається перешкодити доступу до сервісу законних користувачів шляхом перевантаження мережі або сервера. Подумайте, як ви зазвичай потрапляєте на сайт. Більшість основних сайтів здатні обслуговувати мільйони користувачів. Але для цього прикладу, уявіть, що ваш сайт може обслуговувати лише 10 користувачів. Якби хтось провів атаку "відмова в обслуговуванні", то зміг би просто забрати всі 10 місць і законним користувачам було б відмовлено в доступі до сервісу, бо для них не лишилося б місця.



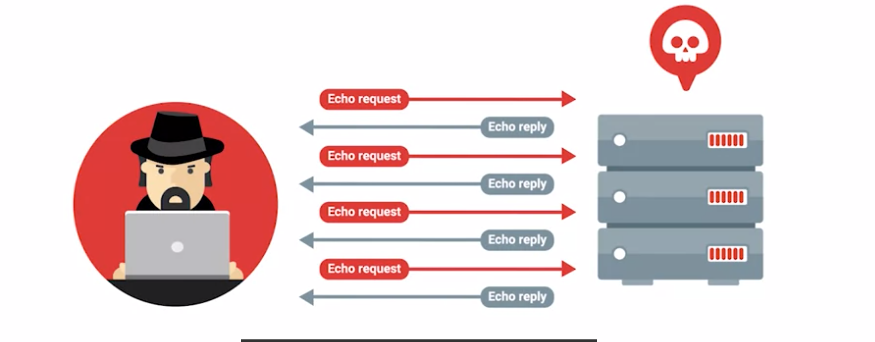
Тепер застосуйте це до такого сайту, як Google чи Facebook. DoS-атаки намагаються зайняти такі ресурси сервісу й запобігти доступу до нього реальних користувачів. Невесела картина.

"Ping of death" (або POD) – досить простий приклад DoS-атаки. Ця атака надсилає на комп’ютер запит ping неправильного формату.



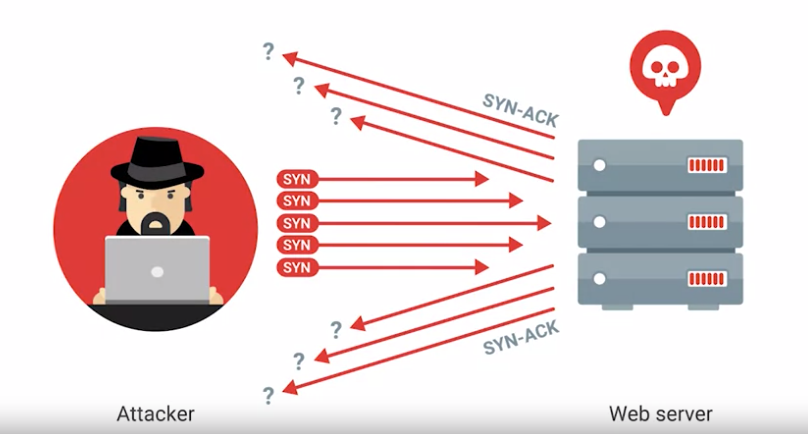
Розмір цього запиту більший, ніж може обробити інтернет-протокол. Як наслідок, виникає переповнення буфера. Це може призвести до збою системи й потенційного виконання зловмисного коду.

Іншим прикладом є атака ping-флуд, що надсилає в систему безліч пакетів ping. Зокрема, вона надсилає ехо-запити ICMP, адже запит ping очікує рівної кількості ехо-відповідей ICMP.



Якщо комп’ютер не може впоратися з цим, може виникнути його перевантаження і збій. Це недобре, ping-флуд, недобре!

Подібно до ping-флуду працює й SYN-флуд. Згадайте: щоб установити TCP-з’єднання, клієнт надсилає пакет SYN на сервер, до якого хоче під’єднатися. Далі сервер надсилає зворотне повідомлення SYN-ACK, після чого клієнт надсилає повідомлення ACK. Під час атаки SYN-флуд сервер піддається бомбардуванню SYN-пакетами. Сервер надсилає назад пакети SYN-ACK, але зловмисник не надсилає повідомлення ACK.



Це означає, що з’єднання залишається відкритим і забирає ресурси сервера. Інші користувачі не зможуть під’єднатися до сервера, що є великою проблемою. Оскільки TCP-з’єднання напіввідкрите, ми називаємо атаки SYN-флуд напіввідкритими атаками. Не дуже зрозуміло, правда? Так і є.

DoS-атаки, які ми вже розглядали, використовують лише один комп’ютер для проведення атаки. Але що, якби зловмисники могли використовувати кілька комп’ютерів? У набагато страшнішому сценарії вони могли б викликати збої в сервісах у більших обсягах і ще швидше. Що ще страшніше, зловмисники справді можуть це зробити. DoS-атака з використанням кількох систем називається розподіленою атакою "відмова в обслуговуванні" (DDoS). Для проведення DDoS-атаки потрібна велика кількість систем, і в цьому зазвичай допомагають ботнети. У цьому сценарії зловмисники можуть отримати доступ до великої кількості комп’ютерів для проведення атаки. У жовтні 2016 року сталася DDoS-атака, мішенню якої став DNS-провайдер Dyn. Підроблені запити на пошук за DNS разом із SYN-флудом, що поширювались через ботнети, перевантажили системи провайдера. Компанія Dyn обслуговувала DNS для великих сайтів, як-от Reddit, GitHub, Twitter тощо. Тож збій її систем одразу вплинув на клієнтів, зробивши ці сервіси недоступними. Не створюйте людям проблем у спілкуванні в Reddit чи Twitter. З власного досвіду знаю: це не дуже добре.

<https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn>

## **Інші атаки**

### **Атаки на стороні клієнта**

Ми багато говорили про атаки, безпосередньо націлені на жертв, але це не єдиний тип атак, які відбуваються в Інтернеті. Можливо, колись ви займатиметеся розробкою ПЗ чи програмуванням, і вам потрібно буде знати про такі види атак, щоб забезпечувати захист своїх продуктів. Поширеним експлойтом безпеки, який може мати місце під час розробки ПЗ і швидко поширюватися мережею, є вставлення зловмисником шкідливого коду. Атаки такого типу ми називаємо "ін’єкційними". Як працюють ін’єкційні атаки? Чудове запитання.

Для простоти ми не вдаватимемось у подробиці впровадження коду, а уявимо собі автомобіль. Щоб автомобіль їхав, ви заливаєте в нього бензин. Тепер уявімо, що хтось хоче заподіяти шкоду цьому автомобілю. Він може залити у ваш бензобак полунично-банановий молочний коктейль. Це звучить смачно, але може вивести автомобіль із ладу. Тож як із цим боротися? Гіпотетично ви можете запобігти цьому, додавши в автомобіль певний механізм, який прийматиме лише бензин, але не інші рідини. Ін’єкційні атаки на сайтах працюють точно так само, але без апетитних полунично-бананових молочних коктейлів і без надмірно складних рішень.

Ін’єкційним атакам можна запобігати завдяки надійним принципам розробки ПЗ, наприклад перевірці вхідних даних і очищенню даних. Хтось ще голодний? Зробимо перерву на молочний коктейль? Ні? Гаразд, рухаймося далі.

Міжсайтовий скриптинг (або XSS-атаки) – це різновид ін’єкційних атак, де зловмисник може вставляти шкідливий код, націлений на користувача сервісу. XSS-атаки – це поширений метод перехоплення сеансів. Для цього можна просто вбудувати зловмисний сценарій у сайті, щоб користувач несвідомо запустив його у своєму браузері. Цей сценарій може виконати шкідливі дії, як-от викрасти файли cookie жертви чи отримати доступ до даних для входу на сайт. Ммм, печиво.

Ще один різновид ін’єкційної атаки – це "SQL-ін’єкція". На відміну від XSS-атаки, що націлена на користувача, SQL-ін’єкція націлена на весь сайт, якщо він використовує базу даних SQL. Зловмисники потенційно можуть запускати команди SQL, які дозволять їм видаляти дані сайту, копіювати їх і виконувати інші зловмисні команди. А тепер, коли ми закінчили, можна й перекусити.

### **Атаки з метою зламу пароля**

Що би хто не казав, але паролі – найнадійніший стандартний засіб безпеки для запобігання несанкціонованому доступу до облікових записів. На жаль, іноді наші паролі не настільки безпечні або надійні, як це потрібно.

Поширеною атакою для отримання доступу до облікового запису є атака на пароль. Атаки на пароль використовують такі програми, як зламувачі паролів, які намагаються вгадати ваш пароль. І вони працюють дуже ефективно, тож не використовуйте скрізь один пароль FIDO. Він не захистив ваш банківський рахунок, не спрацює і тут. Гаразд, рухаймося далі.

Поширеною атакою на пароль є атака методом "грубої сили", яка намагається підібрати пароль, пробуючи різні комбінації символів, доки нарешті не отримає доступ. Оскільки ця атака вимагає випробовування багатьох комбінацій паролів, зазвичай вона триває довго.

Бачили колись CAPTCHA під час входу на сайт? CAPTCHA використовується, щоб відрізнити людину від комп’ютера. Цей метод запитує вас, чи ви людина, чи ви робот або чи ви танцюрист. Під час атаки паролем, якщо на сайті немає CAPTCHA, автоматизована система може намагатися увійти у ваш обліковий запис, доки не підбере правильну комбінацію символів пароля. Але CAPTCHA перешкоджає таким атакам.

Наступний тип атаки на пароль – "перебір за словником". Перебір за словником не випробовує комбінації "грубої сили", як-от abc1 або ABC1. Натомість він випробовує слова, які часто використовуються в паролях, як-от password, monkey, football. Найкращий спосіб запобігти атаці на пароль – використовувати надійні паролі. Не вживайте справжні слова, що містяться в словнику, і обов’язково використовуйте комбінацію великих і малих літер та символів. Без таких заходів безпеки, як CAPTCHA чи інших засобів захисту облікового запису, типовий зламувач паролів приблизно за хвилину зламає такий пароль, як sandwich. Але йому знадобиться значно більше часу, щоб зламати пароль, який ви бачите на екрані, а саме: s@nDwh1ch. Як бачите, це майже те саме, але цей пароль набагато важче зламати.

### **Оманливі атаки**

Приготуйтеся, бо зараз ми поговоримо про одну з найменш технічно складних, але найбільш дошкульних атак, а саме про "соціальну інженерію". Соціальна інженерія – це метод атаки, який спирається насамперед на взаємодію з людьми, а не комп’ютерами. Ви можете скільки завгодно посилювати засоби захисту. Ви можете витрачати мільйони доларів на найсучаснішу інфраструктуру безпеки. Але якщо системна адміністраторка Сьюзен має повний доступ до вашої системи і в неї обманом виманять її облікові дані, ви ніяк не зможете це зупинити.

Як ми знаємо з найкращих науково-фантастичних фільмів, люди – завжди найслабша ланка в житті, і у вашій системі безпеки також. Соціальна інженерія – це своєрідна аферистська гра, де зловмисники обманними методами намагаються отримати доступ до особистої інформації. Потім вони намагаються змусити користувача виконати певну дію і, по суті, обманом змушують жертву це зробити.

Популярним видом атак соціальної інженерії є фішингова атака. Фішинг зазвичай відбувається, коли жертві надсилається зловмисний електронний лист, замаскований під щось законне. Одна з поширених фішингових атак – електронний лист, що повідомляє про злам вашого банківського рахунку й містить посилання для скидання пароля. За цим посиланням ви переходите начебто на сайт свого банку, але насправді він підробний. Таким чином, вас обманом змушують ввести ваш дійсний пароль і облікові дані, щоб скинути дійсний пароль.

Ще одним різновидом фішингу є цільовий фішинг. Обидві ці фішингові схеми мають однакові кінцеві цілі, але цільовий фішинг націлений на конкретну особу або групу. Фейкові електронні листи можуть містити деякі особисті дані,  як-от ваше ім’я, імена ваших друзів чи родичів. Так вони здаються надійнішими.

Ще одна популярна атака соціальної інженерії – спуфінг електронної пошти. Спуфінг – це коли відправник маскується під щось інше. Як виглядає спуфінг? Це відбувається, коли ви отримуєте електронний лист із підробленою адресою відправника. Ви можете надіслати електронний лист, який начебто походить із будь-якого місця – реального чи ні. Уявіть, що ви відкриваєте електронний лист начебто від вашого друга Браяна. На початку листа буде справжня адреса Браяна, а сам лист закликатиме вас переглянути це смішне посилання. Ви знаєте Браяна. Він чудовий хлопець і завжди надсилає дуже смішні листи, тож ви натискаєте посилання. Раптом ви розумієте, що встановили зловмисну програму. І вже, мабуть, не так добре думаєте про Браяна.

Не всі атаки соціальної інженерії відбуваються цифровим шляхом. Одна з таких атак відбувається через фактичний фізичний контакт. Це так званий "бейтинг", що використовується,  щоб змусити жертву щось зробити. Наприклад, зловмисник може просто залишити десь USB-накопичувач, сподіваючись, що хтось під’єднає його до комп’ютера й подивиться, що на ньому. Але цей хтось встановить зловмисну програму, навіть не знаючи про це.

Ще одна популярна атака, яка можлива без інтернет-з’єднання, – "тейлгейтинг", тобто отримання доступу до забороненої зони або будівлі, проходячи за справжнім працівником. У більшості корпоративних середовищ доступ до будівель обмежується за допомогою карток-ключів тощо. Але зловмисник, використовуючи тактику соціальної інженерії, може змусити працівника подумати, що він тут із законною метою, наприклад для обслуговування будівлі або доставки посилок. Потрапивши всередину, зловмисник отримує доступ до корпоративних активів.

Ми поговорили про досить страшні речі, чи не так? Ви, мабуть, і не знали, що існує стільки способів зламати систему безпеки. Сподіваюся, ви краще зрозуміли поширені атаки, а також їхні ознаки, на які слід звертати увагу. Тепер, коли ви дізналися про основні типи загроз безпеці, розгляньмо детально найкращі способи захисту від них, а також як технічно реалізовуються захищені системи. Але спочатку ми перевіримо ваші знання за допомогою тесту, що охоплює різні типи атак, про які ми говорили в цьому модулі.

# **Модуль 2**

## **Симетричне шифрування**

### **Криптографія**

У дитинстві у вас із братами й сестрами була своя секретна мова,

яку не розуміли батьки?

Насправді не мало значення, про що ви говорили.

Головне, щоб батьки про це не здогадалися.

Це було весело, чи не так?

У дитинстві це здавалося вам цікавою грою.

Але протягом усього свого існування

люди створювали способи засекретити свої повідомлення від інших.

На цьому уроці ми розглянемо, як це відбувається шляхом

симетричного й асиметричного шифрування та хешування.

Ми також розглянемо, як описати найпоширеніші алгоритми в криптографії

та навчимося вибирати оптимальний криптографічний метод

для конкретного сценарію.

Але перш ніж ми зануримося в нетрі криптографії та дізнаємось

про різні її типи, що існують у додатках,

зупинімося на деяких основних термінах і загальних принципах,

які допоможуть вам зрозуміти, про що йтиметься далі.

Тема криптографії, тобто приховування повідомлень від потенційних ворогів,

існує вже тисячі років.

Вона надзвичайно розвинулася з появою сучасних технологій,

комп’ютерів і засобів телекомунікації.

Шифрування – це акт прийому повідомлення у вигляді відкритого тексту

та застосування до нього спеціального шифру,

щоб на виході отримати спотворене й нерозбірливе повідомлення

у вигляді шифротексту.

Зворотний процес, коли ми беремо незрозуміле повідомлення

й перетворюємо його на читабельний текст, називається дешифруванням.

Наприклад, розгляньмо простий шифр,

де ми підставляємо "е" замість "o" і "o" замість "y".

Ми візьмемо текст "Hello World" і застосуємо до нього наш базовий шифр.

Як гадаєте, який вигляд матиме цільовий шифротекст?

Сподіваюсь, у вас вийшло "Holly Wyrld".

Цей шифротекст досить легко розшифрувати,

оскільки це дуже простий приклад.

Існують набагато складніші й надійніші шифри чи алгоритми,

які ми розглянемо пізніше в цьому розділі.

По суті, шифр складається з двох компонентів:

алгоритму шифрування та ключа.

Алгоритм шифрування – це базова логіка або процедура,

за допомогою якої відкритий текст перетворюється на шифротекст.

Ці алгоритми – це зазвичай дуже складні математичні операції.

Але є й деякі дуже прості алгоритми, які ми можемо докладно розглянути

й для розуміння яких не потрібно бути доктором математичних наук.

Інший основний компонент шифр – це ключ,

який вводить у ваш шифр щось унікальне.

Без ключа будь-хто, хто використовує той самий алгоритм,

міг би декодувати ваше повідомлення, і насправді жодної таємниці не вийшло б.

Отже, підсумуймо: спочатку ви обираєте алгоритм шифрування

для кодування свого повідомлення, а потім вибираєте ключ.

Тепер у вас є шифр, який ви можете застосувати

до повідомлення з відкритим текстом,

щоб отримати шифротекст, готовий до поширення

й надійно захищений від сторонніх очей.

Це не змушує вас почуватися як міжнародний детектив? Зачекайте.

Оскільки основною метою криптографії є захист ваших таємниць

від прочитання невповноваженими особами, було б логічно,

якби принаймні деякі компоненти шифру також зберігалися в таємниці, чи не так?

Ви можете навести аргумент, що зберігання алгоритму в таємниці

захищає ваші повідомлення від шпигунів, і технічно ви матимете рацію.

Це загальне поняття називається "безпека через неясність".

По суті, це означає: якщо ніхто не знає, який алгоритм ми використовуємо

або який загальний принцип безпеки, то ми в безпеці від зловмисників.

Це як сховати ключ від будинку під килимком на вході.

Допоки грабіжник не знає, що запасний ключ сховано під килимком, ви в безпеці.

Але щойно ця інформація розкриється,

уся безпека одразу зникне разом із вашими цінностями.

Тож, вочевидь, не варто надто покладатися на безпеку через неясність

для захисту комунікацій або систем (або будинку, як у нашому прикладі).

Це загальне поняття в криптографії називається "принцип Керкгоффза".

Згідно з цим принципом, криптосистема, або набір алгоритмів

для генерування ключів і операцій шифрування й дешифрування,

які утворюють криптографічний сервіс, має залишатися надійним,

навіть якщо відома вся інформація про систему, крім ключа.

Це означає, що навіть якщо ваш ворог знає точний алгоритм шифрування,

за допомогою якого ви захищаєте свої дані,

він усе одно не зможе відновити відкритий текст

на основі перехопленого шифротексту.

Ви також можете почути іншу назву цього принципу – "максима Шеннона" або

"ворог знає систему".

Означає вона те саме.

Система має залишатися в безпеці, навіть якщо супротивник точно знає,

які системи шифрування ви застосовуєте, доки ключі залишаються захищеними.

Ми вже визначили термін "шифрування", але комплексна дисципліна, яка охоплює

методи кодування й приховування повідомлень від третіх осіб,

називається "криптографія".

Вивченням цих методів займається наука криптологія.

Протилежність цього, тобто пошук прихованих повідомлень

або намагання розшифрувати зашифроване повідомлення,

називається "криптоаналіз".

Ці дві галузі спільно еволюціонували протягом історії,

розроблялися нові шифри й криптосистеми на заміну тим,

які зламувались або виявлялися вразливими.

Один із найбільш ранніх зафіксованих описів криптоаналізу

дав у IX столітті один арабський математик.

Він описував метод частотного аналізу для зламу кодованих повідомлень.

Частотний аналіз – це метод визначення частоти появи літер у шифротексті.

За цим типом аналізу лежить знання про те, що в письмових мовах

певні літери вживаються частіше, ніж інші,

і деякі літери частіше поєднуються між собою, ніж інші.

Наприклад, в англійській мові найчастіше використовуються літери e, t, a та o.

Найчастіше вживані пари з цими літерами: th, er, on і an.

Деякі шифри, особливо класичні перестановочний і підстановочний шифри,

зберігають відносну частоту літер у відкритому тексті.

А тому вони потенційно вразливі для аналізу цього типу.

Під час Першої та Другої світових війн криптографія та криптоаналіз

відігравали дуже важливу роль.

Відбувся перехід від лінгвістичного й частотного аналізу

до аналізу, більше заснованого на математичних принципах.

Це було пов’язано з розробкою складніших і продуманіших шифрів.

Ключовий переломний момент у галузі криптоаналізу

стався під час Другої світової війни,

коли союзники США почали застосовувати складну математику,

щоб зламувати схеми шифрування для обмеження доступу.

Тоді ж уперше почали використовуватися технології автоматизації

криптоаналізу в Блечлі-Парку, Англія.

Перший програмований цифровий комп’ютер під назвою "Колос"

було розроблено саме для допомоги в цій діяльності.

Застосування перших комп’ютерів для зламу криптографії

відчинило двері для величезного стрибка вперед і розробки

ще складніших і продуманіших криптосистем.

Стеганографія – це споріднений метод,

який, утім, виразно відрізняється від криптографії.

Це метод приховування інформації від спостерігачів без її кодування.

Уявіть, що ви пишете повідомлення невидимим чорнилом.

Повідомлення написане відкритим текстом і не потребує декодування,

але текст прихований від сторонніх очей.

Чорнило невидиме, а щоб його побачити, потрібен механізм, відомий одержувачу.

Почати відтворення відео о :7:4 і дотримуватися тексту7:04

До сучасних стеганографічних прийомів належать вбудовування повідомлень

і навіть файлів в інші файли, як-от зображення або відео.

Випадковий спостерігач бачитиме лише фото симпатичного цуценяти.

Але якщо відкрити це зображення в стенографічній програмі,

вона видобуде повідомлення, приховане у файлі зображення.

Що не так секретно, то це те, як цікаво вивчати

всі ці шпигунські штучки, чи не так?

Далі ми поговоримо про конкретні криптографічні методи та системи.