Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій
_____ Ю.В. Кравченко
«_____»_____2021 року

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

галузі знань 17 «Електроніка та телекомунікації»
за спеціальністю 172 «Телекомунікації та радіотехніка»

на тему:

МЕТОД БОРОТЬБИ З АТАКАМИ ДОСТУПУ В СУЧАСНИХ МЕРЕЖАХ

Виконав: студент групи МІТ -41

Моторний Андрій Сергійович _____
(прізвище ім'я по-батькові) (підпис)

Керівник: асистент кафедри мережевих та інтернет технологій

Герасименко Костянтин Васильович _____
(посада, прізвище ім'я по-батькові) (підпис)

Київ 2021

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій
_____ Ю.В. Кравченко

«_____»_____2021 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Здобувачу вищої освіти Моторний Андрій Сергійович
(прізвище, ім'я, по батькові)

1. Тема роботи:

Метод боротьби з атаками доступу в сучасних мережах

затверджена на засіданні кафедри МІТ «4» грудня 2020 р. протокол № _8__
2. Термін здачі закінченої роботи «30» травня 2021 р
3. Вихідні дані до проекту (роботи) сучасні мережі, загрози та кібератаки, технології забезпечення кібербезпеки

4. Зміст пояснювальної записки (перелік питань, що їх потрібно розробити, обсяг – 35-40 стор.)
1. Аналіз стану сучасних мереж та важливості ІТ-безпеки.
2. Огляд кібератак та існуючих рішень щодо забезпечення безпеки
3. Метод боротьби з атаками доступу в сучасних мережах.

5. Перелік графічного матеріалу 8-10 слайдів

Дата видачі завдання _____
Керівник роботи _____
(підпис) (посада, прізвище, ім'я, по батькові)

Завдання прийняв до виконання _____
(підпис) (прізвище, ім'я, по батькові)

РЕФЕРАТ

Об’єкт дослідження: технологія Fail2ban

Мета роботи (проекту): створити метод боротьби оснований на Fail2ban

Методи дослідження: системний підхід, методи порівняння, структурний аналіз.

У спеціальній частині дана характеристика

В роботі проведено аналіз важливості ІТ-безпеки та атак

Запропоновано метод боротьби оснований на Fail2ban від методу грубої сили

Розроблено скрипти для боротьби з атакми доступу

Практичне значення роботи полягає у забезпеченні безпеки підприємств від атак доступу

Результати здійснених у дипломному проекті досліджень можуть бути використані у будь-якій мережі для прокращення захищеності системи

Наукова новизна дослідження полягає у розробці скриптів у додатку Fail2ban

ЗМІСТ

ВСТУП

Інтернет – це глобальна мережа в якій об’єднуються всі комп’ютери світу. Популярність інтернету, як і кількість користувачів, кожен день все більше зростає. Кожна людина може контактувати з іншими людьми по всьому світу не виходячі з дому. Потенціал мережі неосяжний. Кожен день в Інтернеті зароджуються нові технології, які спрямовані на всі аспекти життя людей. Люди зберігають в Інтернеті великий обсяг своєї особистої інформації. Це потрібно їм для роботи, здійснення операцій в Інтернеті та просто поширення особистої інформації своїм знайомим та друзям.

У сучасному Інтернеті мережева безпека має вирішальне значення. Підприємства повинні забезпечити безпечний доступ всім користувачам до своїх ресурсів в будь-який час. Одним із самих важливих напрямків є розробка методу для захисту підприємств від деяких типів атак. При її розробці потрібно розглянути всю структури мереж взагалі. Також, потрібно проаналізувати важливість безпеки та її актуальність. Ще дуже важливим є огляд усіх відомих типів атак та вже існуючих методів боротьби з ними. При розробці методу потрібно враховувати такі фактори, як збільшення надійності мережі, ефективне управління безпекою та захист від постійно еволюціонуючих загроз і нових методів атак.

1 АНАЛІЗ СТАНУ СУЧАСНИХ МЕРЕЖ ТА ВАЖЛИВОСТІ ІТ-БЕЗПЕКИ

1.1 Огляд сучасних мереж

Для аналізу стану сучасних мереж потрібно їх характеризувати та розглянути їх ієрархію[1]. Кожен реальний об’єкт може мати безліч ознак. Одною із самих розповсюджених ознак під час вибору технології, використовуваної для побудови мережі в першу чергу являється її територіальний масштаб. За цим критерієм розділяють на глобальні мережі та локальні мережі. При чому локальні мережі мають більшу швидкість передачі даних, завдяки вищій якості ліній зв’язку.

Відповідно середовищ передачі комп'ютерні мережі розділяють на дротові мережі - такі мережі, в яких канали зв’язку функціонують на основі мідних або оптичних кабелів, та бездротові мережі, тобто мережі, в яких зв’язок базується на технологіях бездротових каналів зв’язку, такі як радіо, лазерні або інфрачервоні канали.

На технологію комп'ютерної мережі, також впливає і тип середовища передачі, так як її протоколи повинні опиратися на надійність з’єднання і швидкість, що може забезпечити канал, а крім того і частоту спотворення бітів інформації в цьому каналі. Також, бездротові мережі виділяють в особливий клас за допомогою ряду специфічних особливостей, таких як звичайний поділ радіосередовища вузлами мережі, що присутні в радіусі дії всеспрямованого передавача або розподіл діапазону радіочастот між мережами різного призначення, наприклад між комп'ютерними і телефонними.

Мережі можна класифікувати в залежності від того, кому призначаються послуги цих мереж. В залежності від того, для якого типу користувачів призначаються послуги мережі їх поділяють на мережі операторів зв'язку та корпоративні мережі.

Мережі операторів зв'язку надають публічні послуги. Клієнтом мережі може стати будь-який індивідуальний користувач або будь-яка організація, яка уклала відповідний комерційний договір на надання тієї чи іншої телекомунікаційної послуги. Звичайними послугами для операторів зв'язку є послуги телефонії, а також надання каналів зв'язку в оренду тим організаціям, які збираються будувати на їх основі власні мережі. З поширенням комп'ютерних мереж оператори зв'язку істотно розширили спектр своїх послуг, додавши доступ в Інтернет, послуги віртуальних приватних мереж, веб-хостинг, електронну пошту та IP-телефонію, а також широкомовну розсилку аудіо- та відеосигналів. Кожен оператор за збої в роботі своєї мережі несе пряму матеріальну відповідальність, існує таке неформальне поняття, як «обладнання операторського класу», що дає гарантію високих показників надійності, керованості і продуктивності такого обладнання.

Корпоративні мережі надають свої послуги тільки для співробітників підприємств, які володіють цими мережами. Формально корпоративна мережа може мати будь-який розмір, часто під корпоративною розуміють мережу великого підприємства, яка складається з локальних мереж об’єднаних глобальною мережею.

Незважаючи на відмінності між комп'ютерними, радіо, телефонними, телевізійними і первинними мережами, вони мають багато спільного в своїй структурі. У загальному випадку такі телекомунікаційні мережі складаються з термінального обладнання для взаємодії з користувачами, магістральної мережі, мереж доступу, центрів управління сервісами або інформаційних центрів її можна побачити на рисунку 1.1.

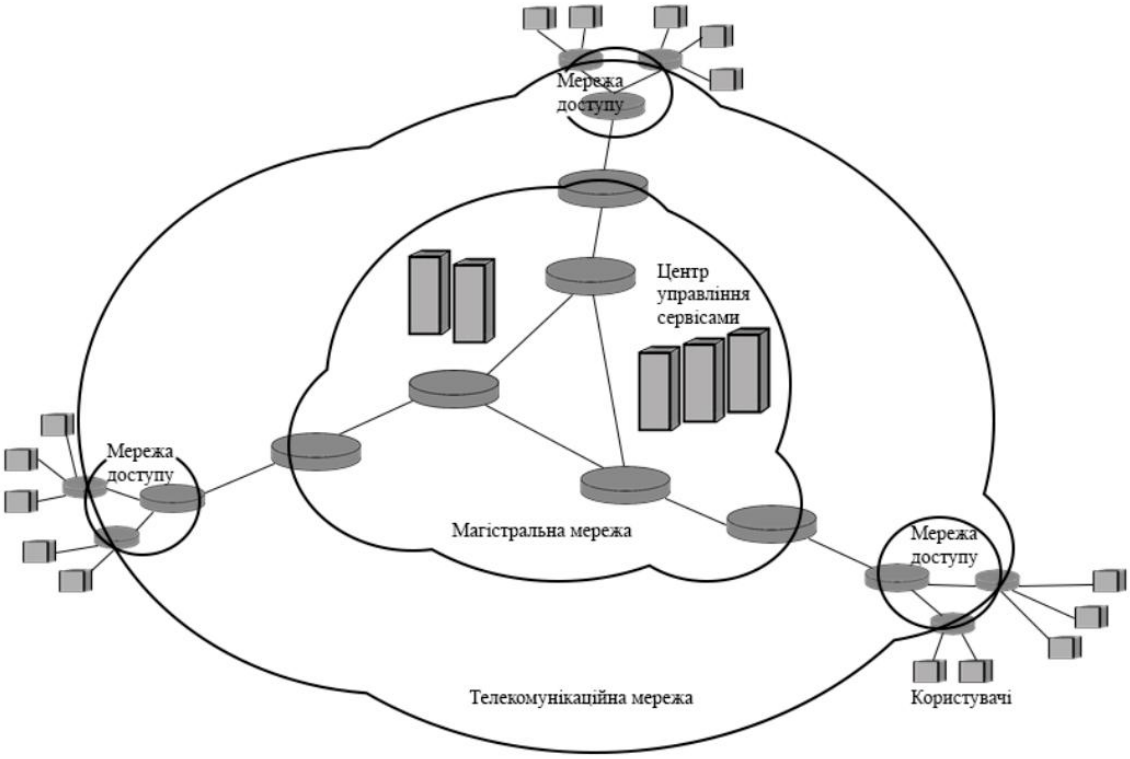

Рис 1.1 – Схема телекомунікаційної мережі

Мережа доступу являється регіональною мережею, що вирізняється великою розгалуженістю. Як і телекомунікаційна мережа в цілому, мережа доступу має декілька рівнів. Комутатори, які встановлені в вузлах нижнього рівня, мультиплексують інформацію, що рухається по чисельним абонентським каналам, часто званим абонентськими закінченнями, і передають її комутаторам верхнього рівня, а ті, в свою чергу, передають її комутаторам магістралі. Кількість рівнів мережі доступу прямо пропорційна її розміру. Мережа доступу не великих масштабів може складатися тільки з одного рівня, а більша - з двох або трьох.

В магістральній мережі об’єднуються окремі мережі доступу, яким забезпечено між собою транзит трафіку по високошвидкісних каналах.

Комутатори магістралі оперують не лише інформаційними з'єднаннями між окремими користувачами, а також і агрегованими інформаційними потоками, які керують даними великої кількості з’єднань призначених для користувача. В результаті цієї передачі інформація по магістралі потрапляє в мережу доступу одержувачів, в якій вона спочатку демультиплексируется, а

потім комутується таким чином, щоб на вхідний порт обладнання користувача потрапляла тільки адресована конкретно йому інформація.

Інформаційні центри або центри управління сервісами, забезпечують інформаційні послуги в мережі. В таких центрах може зберігатися користувацька інформація, тобто така інформація, що безпосередньо призначена для кінцевих користувачів мережі та допоміжна службова інформація, яка призначена для допомоги постачальнику послуг в наданні послуг користувачам.

Прикладом інформаційних ресурсів призначених для користувача можуть служити веб-портали, на яких розташована різноманітна довідкова і новинна інформація, інформація електронних магазинів. У телефонних мережах інформаційні центри надають послуги екстреного виклику і довідкові послуги різних організацій і підприємств.

До інформаційних центрів, що зберігають ресурси другого типу можна віднести різні системи аутентифікації та авторизації користувачів, за допомогою яких організація володіюча мережею, перевіряє права користувачів на отримання певних конфіденційних даних; системи білінгу, які в комерційних мережах характеризують плату за отримані послуги; бази даних імен і паролів, а також переліки послуг, на які підписаний користувач.

В залежності від призначення і розміру мережі, в ній можуть бути відсутні або ж мати неістотне значення деякі складові загальної структури.

В кібербезпеці найбільшу увагу приділено корпоративній мережі. Це мережа підприємства, яка може мати будь-які масштаби, але зазвичай так називають мережу великого підприємства з децентралізованою структурою розташування відділень. Корпоративна мережа являє собою складену мережу, що містить в собі локальні і глобальну мережі. Прийнято ділити корпоративну мережу на мережі відділів і робочих груп, мережі будівель і кампусів, магістраль.

Мережі відділів використовуються в межах одного відділу підприємства невеликою групою співробітників. В даному відділі співробітники працюють

над вирішенням деяких загальних завдань, таких як ведення бухгалтерського обліку або маркетинг. Стандартом можна вважати, 100-150 співробітників в одном відділі.

Основним призначенням мережі відділу є розподіл локальних ресурсів, таких як додатки, дані і модеми. Мережі відділів не розділяють на підмережі, вони мають в своєму складі один або два файлових сервера і не більше тридцяти користувачів. Велика кількість трафіку підприємства локалізується у цій мережі, що забезпечує кращий контроль над інформацією підприємства. Мережі відділів зазвичай створюються на базі мережевої технології, такої як Ethernet, Token Ring або FDDI.

Основним керуючим лицем в мережах відділу є мережевий адміністратор. До його завдань на рівні відділу належить інтегрування нових користувачів до мережі підприємства, усунення неполадок в системі, забезпечення доступності обладнання, проведення найпростіших заходів для забезпечення безпеки мережі, установка нових вузлів і нових версій програмного забезпечення. Такою мережею може управляти співробітник, присвячує обов’язкам адміністратора тільки частину свого часу. Найчастіше адміністратор мережі відділу не являється спеціалістом у сфері кібербезпеки, але є тією людиною у відділі, який краще за всіх розбирається в комп’ютерах, і займається адмініструванням мережі та може проводити лікбез для інших співробітників для роботи з обладнанням та найпростішими принципами захисту конфіденційної інформації.

Мережі робочих груп близькі до мереж відділів. До них відносять зовсім невеликі мережі, які включають до 15-20 комп’ютерів. Мережі робочих груп мають майже такі самі характеристики, що і мережі відділів. Але такі властивості, як простота мережі і однорідність, тут проявляються найбільшою мірою.

Мережа будівлі являється об’єднанням мережі різних відділів одного підприємства в межах окремої будівлі, а мережа кампуса в межах однієї території площею в кілька квадратних кілометрів. Мережі будівель

будуються на основі технологій локальних мереж, їх можливостей достатньо для забезпечення необхідної зони покриття.

Зазвичай мережа будівлі будується за ієрархічним принципом, вона має власну магістраль, побудовану на базі технології Gigabit Ethernet, до неї за допомогою технології Fast Ethernet або Ethernet приєднуються мережі відділів.

Така мережа надає послуги достатні для взаємодії мереж відділів між собою, доступу до загальних баз даних підприємства, доступу до загальних факс-серверів, високошвидкісних принтерів і високошвидкісних модемів. В цій мережі співробітники кожного відділу підприємства можуть отримати доступ до деяких ресурсів і файлів мереж інших відділів підприємства. Важливою властивістю, яка притаманна мережам кампусів, є надання доступу до корпоративних баз даних незалежно від типу комп’ютерів, на яких ці бази розташовуються. Саме на рівні мережі кампуса можуть виникати проблеми інтеграції неоднорідного апаратного та програмного забезпечення.

В корпоративній мережі на перший план виходить надання інформаційних послуг. Кожен розробник і фахівець з обслуговування корпоративних мереж повинен враховувати, що невід’ємною частиною таких мереж є настільні комп’ютери користувачів і сервери.

Обов’язковим у корпоративних мережах є використання різних типів комп’ютерів - від мейнфреймів до персональних комп'ютерів, різних типів операційних систем та безліч різних додатків. Основним принципом корпоративної мережі є, що її неоднорідні частини повинні працювати як єдине ціле та надавати користувачам зручний і простий доступ до всіх необхідних ресурсів, підтримуючи доступність інформаційних систем і послуг.

В локальній базі облікових даних кожного комп’ютера розміщено облікові дані всіх користувачів, до цих ресурсів мають мати доступ ці користувачі та користувачі з відповідним рівнем дозволу. При спробі доступу дані спочатку дістаються з локальної облікової бази і на основі цих

даних доступ надається або не надається. Цей підхід добре працює тільки в невеликих мережах обсягом 5-10 комп’ютерів. При наявності в мережі великої кількості користувачів, близько кількох тисяч, кожному з яких потрібен доступ до великої кількості серверів використовується централізована довідкова система, яка містить в собі базу даних з обліковими записами всіх користувачів системи. По мережі циркулюють великі обсяги даних, тому мережа повинна забезпечити їх безпеку і захищеність поряд з доступністю. При побудові корпоративних мереж використовуються найбільш потужне і різноманітне обладнання та програмне забезпечення, так для аналізу найсучасніших методів кібербезпеки краще розглядати, саме корпоративні мережі.

Інтернет неухильно рухається до того, щоб стати загальносвітовою мережею інтерактивної взаємодії людей. Він починає все більше і більше використовуватися не тільки для поширення інформації, в тому числі рекламної, але і для здійснення ділових операцій - покупки товарів і послуг, переміщення фінансових активів.

Інтернет є мережею, яка не має єдиного центру управління і в той же час працює за єдиними правилами і надає всім своїм користувачам єдиний набір послуг. Інтернет - це «мережа мереж», але кожна вхідна в Інтернет мережа управляється незалежним провайдером. Деякі центральні органи існують, але вони відповідають тільки за єдину технічну політику, за узгоджений набір технічних стандартів, за централізоване призначення таких життєво важливих для гігантської складової мережі параметрів, як імена та адреси комп'ютерів і входять в інтернет мереж, але не за щоденне підтримання мережі в працездатному стані. Така висока ступінь децентралізації має свої переваги і недоліки.

Переваги проявляються, наприклад, в простоті розширення Інтернету. Новий постачальник послуг просто укладає угоду, принаймні, з одним з існуючих провайдерів, після цього користувачі нового постачальника отримують доступ до всіх ресурсів Інтернету. Негативні наслідки

децентралізації полягають у складності модернізації технологій і послуг Інтернету. Інший приклад - не дуже висока надійність послуг Інтернету, так як ніхто з постачальників не відповідає за кінцевий результат.

Інтернет не став би тим, чим він став, якби не ще одна його унікальна риса - неосяжне інформаційне наповнення і простота доступу до цієї інформації для всіх користувачів Інтернету, що є як його перевагою, так і недоліком, так як в Інтернеті інформація не фільтрується і немає гарантій її достовірності. Багато людей сьогодні не уявляють свого життя без регулярного використання Інтернету і для листування зі знайомими, і для пошуку інформації, і для пошуку роботи, і для оплати рахунків, і для шахрайства.

1.2 Аналіз стану мереж

Інтернет постійно розвивається та на даний час є глобальною мережею в якій люди можуть взаємодіяти між собою в реальному часі. Професійне життя людей перебирається в Інтернет. Інформація підприємств та звичайних людей оцифровується та зберігається в цій мережі. Люди не тільки поширюють інформацію, але і здійснюють ділові операції, такі як покупки товарів або послуг, робота з активами.

Сучасна мережа Інтернет не має якогось одного центру управління, але при цьому підпорядковується єдиним правилам, а всі користувачі мережі мають єдиний набір послуг. Унікальною рисою Інтернету є безкінечне наповнення інформацією та простота доступу до неї всім бажаючим.

В Інтернеті існує велика кількість груп даних, які утворюють різні домени. Такі групи можуть збирати та обробляти велику кількість даних і від обсягу цих даних залежить сила і вплив доменів. Ці дані можуть бути у вигляді чисел, зображень, відео, аудіо або у вигляді будь-якого типу даних, який може бути поданий у цифровій формі. Найпотужніші групи можуть діти як окремі області мережі Інтернет.

Такі компанії, як Google, Facebook і LinkedIn, можуть вважатися доменами даних в мережі Інтернет. Люди, які працюють в цих компаніях, можуть вважатися експертами з кібербезпеки.

Слово домен має велику кількість значень. Будь-яка область, де існує контроль, авторизація або захист, можна вважати доменом. Домени розглядаються як області, які підлягають захисту. Вони можуть бути обмежені логічною або фізичною межею. Це буде залежати від розміру задіяної системи. У багатьох аспектах, експерти в області кібербезпеки, повинні захищати свої домени відповідно до законів своєї країни.

Експерти Google створили один з перших і найпотужніших доменів у відкритому Інтернеті. Мільярди людей щоденно використовують Google для пошуку в Інтернеті. Ймовірно Google, створив найбільшу в світі інфраструктуру збору даних. Операційна система розроблена цією компанією встановлену на більше, ніж 80% всіх мобільних пристроїв, підключених до Інтернету. Кожен пристрій вимагає від користувачів створення облікових записів Google, які можуть зберігати закладки та інформацію про обліковий запис, результати пошуку та навіть знаходити пристрій.

Потужним домен у доступному Інтернеті є Facebook. Експерти в Facebook виявили, що люди щодня створюють персональні облікові записи для спілкування з родиною та друзями. Роблячи це, вони добровільно надають значний обсяг особистих даних. Експерти Facebook створили величезний домен даних, який дозволяє людям спілкуватися і знайомитися використовуючи способи, які не можна було уявити в минулому. Facebook щоденно впливає на мільйони людей і дозволяє компаніям та організаціям спілкуватися з людьми більш персоналізовано і цілеспрямовано.

LinkedIn являється ще одним доменом зберігання даних в Інтернеті. Учасники цієї мережі діляться інформацією про свої досягнення з метою створення мережі професійних контактів. Користувачі LinkedIn надають

інформацію для створення онлайн-профілів і контактів з іншими учасниками цієї соціальної мережі. LinkedIn сприяє зв'язкам працівників з роботодавцями, а компаніям зв’язок з іншими компаніями у всьому світі.

Якщо заглянути в середину цих доменів, то можна зрозуміти, як вони побудовані. На базовому рівні ці домени є потужними через здатність збирати дані, які надаються самими користувачами. Ці дані часто включають в себе біографічні дані користувачів, їх коментарі, місця, що були відвідані, подорожі, інтереси, друзів і членів сім’ї, професію, хобі, а також робочий і особистий графік. Для організацій, що зацікавлені у використанні цих даних для кращого розуміння і спілкування з своїми клієнтами та співробітниками, така інформація має велику цінність.

Дані, які зібрані в Інтернеті, містять значно більше відомостей, ніж ті дані, які користувачі надають добровільно. Домени продовжують рости відповідно до розвитку науки і техніки, дозволяючи експертам і їх роботодавцям збирати багато інших видів даних.

З’явилися нові технології, такі як геопросторові інформаційні системи. Ці нові технології можуть відслідковувати стан дерев в районі. Вони можуть надавати актуальну інформацію про розташування транспортних засобів, пристроїв, людей і предметів. Цей тип інформації може заощадити енергію, підвищити ефективність і знизити ризики у сфері безпеки. Кожна з цих технологій також викличе різке збільшення обсягу зібраних, проаналізованих і використаних даних, з метою розширення знань про оточуючий світ. Дані, що збираються GIS і IoT, будуть створювати величезну проблему для експертів з кібербезпеки в майбутньому. Потенційно типи даних, які генеруються цими пристроями, можуть дозволити кіберзлочинцям отримати доступ до дуже особистих аспектів повсякденного життя.

1.3 Аналіз важливості IT-безпеки

Велику актуальність в сучасному Інтернеті має важливість інформаційної безпеки. Сучасні проблеми виявляються великою кількістю факторів. По даним порталу статистичних ринкових даних Statista, в самих провідних компаніях у зв'язку з порушенням інформаційної безпеки налічуються збитки на суму, яка становить мільярди євро, і це тільки враховуючи, що тільки третина із усіх опитуваних компаній змогли визначити кількісний розмір втрат.

Швидкі темпи розвитку прогресу інформаційних технологій в цілому значно обходять по цим параметрам темпи розвитку технологій мережевої безпеки. А створення технологій, які забезпечують безпеку, та проведення превентивних заходів для убезпечення інформації має прецедентний характер, тобто боротися з деякими загрозами можна тільки після їх виникнення. А вони можуть нанести величезних збитків, як в фінансовому плані, так і в репутаційному.

Ще одним фактором важливості безпеки є різке збільшення числа користувачів по всьому світу і при цьому зберігається високий контраст комп'ютерної грамотності населення в плані захисту своїх даних. Безграмотних користувачів легко примусити віддати свої персональні дані за допомогою соціальної інженерії.

Значне збільшення обсягу інформації, яка зберігається і обробляється комп'ютерами та іншим обладнанням автоматизації. Породжує і людей, які можуть використати цю інформацію в своїх не зовсім законних цілях. За оцінками експертів, в даний час близько 70-90% інформації та документів компаній зберігаються в цифровому форматі - текстові файли, електронні таблиці, бази даних.

На сучасному етапі розвитку суспільства зростає роль електронних ресурсів, які є не чим іншим, як сукупність даних, інформаційний комплекс, які виконують збір, формування, поширення та використання інформації. При цьому утворюються відносини, які регулюються спеціальними системами.

Зростання в швидкому темпі комп'ютерних технологій в різних сферах життєдіяльності людей має як позитивні наслідки, такі як покращення результатів в даних сферах, так і негативні – воно стало основою для утворення принципово нового сегменту міжнародної злочинності, яка несе небезпеку державам і міжнародній системі взагалі.

Для аналізу сучасної важливості ІТ-безпеки потрібно розглянути приклади порушень безпеки та їх наслідки[2]. Однією із таких подій був інцидент, що стався в 1989-х роках в США, його назвали найбільшим актом порушення безпеки інформаційних систем в Америці за весь час. Студент університету в місті Ітака Роберт Морріс написав і запустив по комп'ютерній мережі ARPANET програмне забезпечення, яке представляло з себе мережевий вірус, комп'ютерний хробак Морріса. Результатом цього було заблоковано роботу американських комп'ютерних мереж, таких як Інтернет, ARPANET, BITnet та деякі інші маючі велике значення для працездатності не тільки громадського життя, а ще і військового. Цим вірусом було вражено більше 6000 комп'ютерів по всій території Америки в найбільших університетах, інститутах, урядових закладах, закладах міністерства охорони здоров'я, військових базах. Це привело до збитків оцінених фахівцями в 100 мільйонів доларів. Самого Морріса було виключено з університету, а він сам став першою людиною, яку арештували відповідно до закону.

Також щоб побачити небезпечність, яку несе розвиток технологій можна розглянути військову операцію «Буря в пустелі» під час її проведення Збройні сили США використовуючи випромінювачі саботували роботу радіо і телефонного зв'язку на всій території Іраку. За допомогою секретних вірусів, які були упроваджені в комп'ютерну систему з пам'яті принтерів, які

до цього були придбані в деякій комерційній фірмі, були виведені із ладу система управління протиповітряної оборони Іраку.

Ще одним прикладом э воєнний конфлікт в Косово, для припинення військової операції Югославська Федерація організувала хакерські атаки на веб-сайти країн НАТО, які підтримували роботоздатність комп'ютерних систем Пентагону. Це призвело до того, що було паралізоване британське метеорологічне бюро, яке не могло надавати необхідні показники для підтримки повітряних атак НАТО, і деякі з них довелось скасувати.

Проблема кіберзлочинів робить очевидним необхідність розробки міжнародно-правових засад, які регулюють взаємовідносини у міжнародному праві, ця сфера зазнає постійних змін під впливом умов забезпечення міжнародної та національної безпеки. З появою нових технологій з'являються і нові злочини. Тому можна виявити основні кримінальні напрямки комп'ютерній діяльності. До них відносять підробку цифрової інформації, пошкодження даних та програм, саботаж комп'ютерних систем, несанкціонований доступ до інформації та порушення авторських прав.

До актуальних проблем важливості ІТ-безпеки проявляється в можливих перешкодах та особливому характері їх сприйняття суспільством, зростаюча тенденція до появи великої кількості злочинців в інформаційній сфері та ряд нерозроблених теоретичних постулатів по інформаційній безпеці. Тому для вирішення цих проблем, було прийнято комплексні міри, які беруть до уваги законодавчі, організаційні та програмно-технічні заходи і засоби. Такі засоби можуть бути інтегровані в операційні системи, або постачатися у форматі окремих програмних забезпечень. Більше уваги приділяють забезпеченню безпеки в операційних системах. Навіть Генеральна Асамблея ООН в 1999 році висунула резолюцію, в якій було висловлено занепокоєність через те, що популяризація та використання новітніх інформаційних технологій і засобів, в перспективі може використовуватися з метою, суперечну з завданнями по забезпеченню міжнародної стабільності та безпеки.

Звичайні користувачі повинні бути обережними користуючись новими програмними додатками, адже вони мають чисельні уразливості в програмному забезпеченні і мережевих платформах. Через конкуренцію сучасні програмні продукти надходять у продаж з помилками і недоліками. Розробники включають в продукт велику кількість функцій, але у них немає часу на налагодження і тестування створених систем. Помилки і упущення, що залишаються в цих системах, призводять до випадкових і навмисних порушень інформаційної безпеки.

Швидкий розвиток Інтернету сприяє порушенням безпеки систем обробки інформації в усьому світі. Глобалізація дозволяє хакерам здійснювати атаку на корпоративну мережу з будь-якої точки світу, де є Інтернет, не маючи фізичного доступу. Тому забезпечення безпеки комп'ютерних систем і мереж є одним з провідних напрямків розвитку інформаційних технологій.

2 ОГЛЯД КІБЕРАТАК ТА ІСНУЮЧИХ РІШЕНЬ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

2.1 Поняття кібербезпеки та кіберзлочинців

Інтернет – це всесвітня мережа, яка об’єднує всі світові комп’ютери, дає змогу людям контактувати між собою з різних точок планети. Він має неосяжний потенціал, а технологій в середині нього стає все більше. Із зростанням популярності мережі Інтернет в ньому з’являється все більше користувачів, але не всі заходять сюди з добрими намірами. В зв’язку з цим закономірно в Інтернеті зародилась кібербезпека[3]. На початку єри Інтернет кіберзлочинці були підлітками або аматорами, які проводили атаки зі своїх домашніх комп’ютерів для забави. Але сучасний світ кіберзлочинців сильно виріс та став набагато небезпечнішим. Нападниками може бути особа або група особ, які намагаються використати вразливості для особистої або фінансової вигоди. Ці злочинці зацікавлені у всьому, від кредитних карток до дизайну продукту та будь чому, що має цінність.

Кіберзлочинців можна поділяють на три типи. Найневинніший тип це аматор, який практично не має навичків та працює в основному за інструкцією в Інтернеті. Вони використовують базові інструменти, але результати можуть бути руйнівними. Наступним типом є хакери, які взламують мережі з метою отримання доступу. Хакери можуть класифікуються як білі, сірі або чорні. Перший тип хакерів втручаютсья в комп’ютерну систему або мережу, щоб виявити слабкі місця та покращити безпеку цих систем. Власники системи дають дозвіл на виконання проникнення і отримують результати тесту. З іншого боку, чорні хакери використовують будь-яку вразливість для незаконної особистої, фінансової або політичної вигоди. Сірі хакери знаходяться десь посередині між білими та чорними. Хакери у сірих капелюхах можуть виявити вразливість і

повідомити власникам системи, якщо це збігається з їхніми планами. Деякі сірі капелюхи публікують факти про вразливість в Інтернеті, щоб інші нападники могли її використовувати. Також є організовані хакери. До таких хакерів відносяться організації кіберзлочинців, хактивісти, терористи та хакери, що фінансуються державою. Кіберзлочинці зазвичай є групами професійних злочинців, орієнтованих на контроль, владу та багатство. Ці злочинці дуже витончені та організовані і вони навіть можуть надавати кіберзлочинність, як послуги іншим злочинцям. Хактивісти роблять політичні заяви, щоб проінформувати про важливі для них питання. Вони також публікують негативну інформацію про своїх жертв. Нападники, які фінансуються державою, здійснюють розвідку чи саботаж від імені свого уряду. Деякі хакери, які фінансуються державою, перебувають на службі у збройних силах своєї держави.

Загрози, вразливості та атаки є центром уваги фахівців у галузі кібербезпеки. Загроза - це можливість того, що може відбутися небезпечна подія, яка призведе до втрат, наприклад атака. Вразливість - це вада, яка робить ціль атаки сприйнятливою до нападу. Атака - це навмисне використання виявлених вразливостей комп'ютерних інформаційних систем як з конкретною метою, так і просто для розваги. У кіберзлочинців можуть бути різні мотиви для вибору цілі атаки. Вони постійно шукають та виявляють вразливі системи. Зазвичай жертвами стають системи, на яких не встановлені оновлення або відсутній захист від вірусів і спаму.

2.2 Загроза шкідливого програмного забезпечення та зловмисний код

Фахівці з кібербезпеки повинні розуміти алгоритм реалізації кожної з атак, яку вразливість вона використовує і яким чином це впливає на жертву. Кібератаки - це тип нападу, який використовується кіберзлочинцями на

цільові комп'ютерні системи, мережі та інші комп'ютерні пристрої. Зловмисники атакують як дротові так і бездротові мережі.

Зловмисне програмне забезпечення або шкідливе ПЗ - це термін, який використовується для опису програмного забезпечення, призначеного для порушення роботи комп'ютера або отримання доступу до комп'ютерних систем без відому або дозволу користувача. Зловмисне програмне забезпечення стало загальним терміном, який використовується для опису всіх ворожих або нав'язливих програм. Термін "зловмисна програма" описує комп'ютерні віруси, черв'яки, троянські коні, програми-вимагачі, шпигунські програми, рекламне програмне забезпечення, псевдоантивіруси та ін. Деяке шкідливе ПЗ виявити легко, дію інших виявити практично неможливо. Кіберзлочинці досягають кінцевих пристроїв користувача, встановлюючи на них зловмисне програмне забезпечення.

Вірус являє собою шкідливе програмне забезпечення, яке прикріпляється до виконуваного файлу, будь-якої легітимної програми. Майже всі віруси потребують попередього запуску зараженої програми від користувача, але є і такі, що можуть активуватися в конкретний час або дату. Комп'ютерні віруси зазвичай поширюються одним із трьох способів: через знімні носії; завантажуються з Інтернету; через вкладення електронної пошти. Рівень небезпеки вірусів може варіюватися, вони можуть виводити звичайні рисунки на екран, або призводити до руйнівних наслідків, змінюючи або видаляючи дані. Віруси мають здібності для мутації, що допомагає їм уникати виявлення. Заразитися вірусом можна навіть просто відкривши файл. Деякі віруси вражають завантажувальний сектор або файлову систему флеш-накопичувачів, а з них можуть поширюватися на системний жорсткий диск комп’ютера. Також зараження вірусами може відбуватися при виконанні конкретної програми. Після активації вірусу він постійно заражатиме інші програми на комп'ютері або на інших комп'ютерах в мережі.

Черв’яки – це зловмисний код, вони поширюються самостійно, знаходячи та користуючись вразливостями інфраструктури мережі. Звичайно черв’яки мають ціль сповільнити роботу мережі. Віруси потребують попереднього запуску зараженої програми, а черв’яки не потребують запуску та працюють самостійно. Потрібно тільки первинно інфікувати мережу і далі черв’як не потребує втручання від користувача. Після зараження одного вузла поширення черв’яка проходить з великою швидкістю. Принцип дії черв’яків є єдиним. Вони знаходять певну вразливість, якою користуються, у них присутній механізм розповсюдження та здійснює деяку зловмисну дію.

Троянський кінь, як і інші є зломвисною програмою, яка виконує деструктивні дії під виглядом потрібної операції, наприклад запуску виконуваного файлу програми. Він користується тими ж привілеями, що і користувач, який його запускається. Від віруса від відрізняєтсья тим, що прив’язується до невиконуваних файлів, наприклад мультимедіа або ігри.

Логічна бомба являється програмою шкідником, яка має тригер, що вкористовуєтсья для пробудження зловмисного коду. Активаторами може бути запуск деякої програми, зміна або видалення облікового запису користувача, або просто дата і час. Доки подія-активатор не відбулась логічна бомба залишається не активною та в таком стані не завдає проблем. Руйнівна дія цього програмного забезпечення направлене на пошкодження записів в базі даних, видалення файлів та атака на застосунки та операційні системи. Більш сучасні представники такого ПЗ можуть атакувати та руйнувати апартні компоненти робочих станцій та серверів, такі як процесор, пам’ять, блок живлення та массиви зберігання інформації. Заражені компоненти змушені працювати в критичному режимі, доки вони стануть не працездатними.

Програми-вимагачі – це програмне забезпечення, яке блокує комп’ютерну систему або її складові, доки жертва не заплатить визначений

викуп. Вони зазвичай за допомогою ключа невідомго користувачу шифрують дані на комп'ютері. Для зняття обмежень портібно внести певну грошову суму. Для блокування деяких системи створюються спеціалізовані програми-вимагачі. По аналогії з троянським конем програми-вимагачі розповсюджуються через завантаженя файлів або вразливості ПЗ. За транзакцію оплати жертвою не можливо відслідкувати отримувача, через специфікацію платіжної системи. Після сплати користувач отримує від зловмисника програму, яка розшифровує файли або відсилає ключ для розблокування. Інтерфейс такої програми зображений на рисунку 2.1.

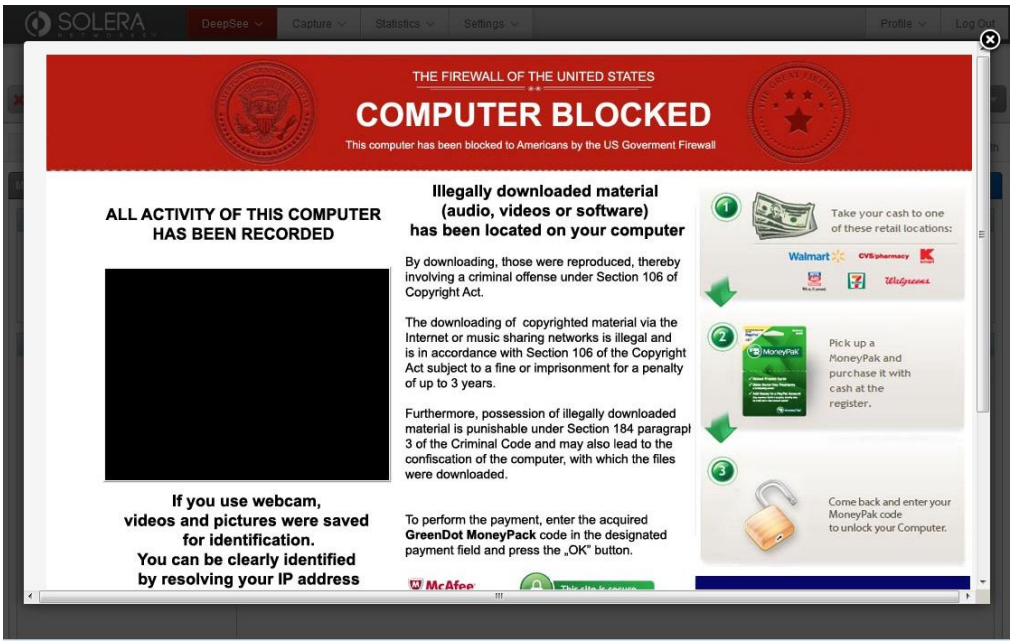

Рис 2.1 – Інтерфейс програми-вимагача

Backdoor – це програма або код, який був доданий зловмисником та скомпроментував систему. Він легко може обійти стандартну аутентифікацію, яка використовується для доступу до системи. Найпоширенішими є такі програми, як Netbus і Back Orifice, вони можуть надавати віддалений доступ до системи неавторизованим користувачам. Основною метою backdoor є надати злочинцю доступ в майбутньому, навіть коли організація уже позбудеться від вразливості, через яку було атаковано систему. Найпоширеніший спосіб зараження злочинцем, це несвідомий

запуск авторизованим користувачем троянської програми на своєму комп’ютері. Руткіт проводить модифікацію операційної системи для створення чорного ходу. Через нього зловисник має віддалений доступ до комп’ютера. Загалом всі руткіти користуються слабкими місцями програмного забезпечення для отримання привілеїв та модифікації системних файлів. Це можливо через недоліки системи або помилки програмування. Ще, руткіти можуть вносити зміни в системи перевірки станів та різні моніторингові системи, що підвищує рівень захищеності програми від виявлення. Іноді щоб позбутися руткіту потрібно повністю переустановити операційну систему.

Електронна пошта являється універсальним сервісом, що мається у використанні у великої кількості людей по всьому світу. Через че, вона стала головною вразливістю для користувачів та організацій. Одним їз ключових понять є спам – небажана пошта. В більшості інциндентах він являється звичайним способом реклами. Але в ньому може міститись шкідливі посилання, зловмисне програмне забезпечення. Метою ебезпечного спаму є роздобути конфіденційну інформацію користувача, наприклад інформацію про банківський рахунок або номер платника податків. Поширювачами спаму є заражені вірусом або черв’яком комп’ютери розташовані в мережах зловмисника. Ці комп’ютери розсилають настільки велику кількість спаму, що навіть сучасні функції захисту від спаму не можуть заблокувати все. До основних характеристиками спаму відноситься відсутня тема листа, електронний лист вимагає оновлення облікового запису, текст листа має помилки або дивну пунктуацію, лист вимагає від користувача відкрити вкладення. Якщо користувач отримує електронний лист, що відповідає одному або декільком з цих характеристик, йому не варто відкривати цей лист або будь-які вкладення. Зазвичай політика використання електронної пошти організації вимагає, щоб користувач, який отримав електронний лист такого типу, повідомив про це співробітникам відділу кібербезпеки. Майже

всі поштові сервіси фільтрують спам. На жаль, спам все одно створює навантаження на мережу і сервер отримувача.

Шпигунське ПЗ - це програмне забезпечення, яке дозволяє злочинцям отримувати інформацію про дії користувача за комп'ютером. Шпигунські програми часто містять засоби відстеження активності, набраних на клавіатурі символів та перехоплення даних. Для того, щоб обійти заходи безпеки, шпигунські програми часто змінюють налаштування безпеки. Шпигунські програми часто прив'язуються до легального ПЗ або розповсюджуються троянами. Багато веб-сайтів, які поширюють умовно-безкоштовні програми, містять шпигунські програми.

Рекламне програмне забезпечення конкретної шкоди не несуть, а просто відображають спливаючі вікна з рекламою, автори яких на меті мають отримання доходу з реклами. Таке програмне забезпечення уміє аналізувати запити користувача його інтереси, та сайти, які він відвідує. На основі цієї інформації з’являється тематична вспливаюча реклама. Найчастіше таке програмне забезпечення встановлюється зі звичайною програмою зібраною користувачем в інтернеті, але може поширюватися разом із шпигунськими ПЗ.

Scareware - це шкідливе ПЗ, яке переконує користувача здійснити конкретну дію, використовуючи його страх. Scareware створює спливаючі вікна, схожі на вікна діалогу операційної системи. Ці вікна містять підроблені повідомлення про те, що система знаходиться під загрозою або необхідно виконання певної програми для повернення до нормальної роботи. Насправді жодних проблем немає і якщо користувач дозволить виконати зазначену програму, вона встановить на його комп'ютер зловмисний код.

Фішинг являє собою форму шахра’ства. Злоцинці, прикидаються організацією чи особою з хорошою репутацією, засобами обміну повідомлення, такими як електронна пошта або месенджери, вони збирають

інформацію про обліковий запис. Фішингом можна звати явище, коли лист надісланий злочинцем має вигляд, як лист з надійного джерела. Його метою є примушення користувача безсумніву встановити, якийсь зловмисний програмний додаток або повідомити свою конфіденційну інформацію. Як приклад можна привести фальшивий електронний лист начебто від магазину або державних органів. В листі надані рекомендації користувачу перейти по посиланню, для отримання призу, зники або внесенню, якихось даних. За посиланням знаходиться сторінка, яка отримує IP-адресу користувача та дані, які він введе.

Спрямований фішинг - це цілеспрямована фішингова атака. Як звичайний, так і спрямований фішинг використовують електронну пошту, щоб досягнути жертв. Але у випадку спрямованого фішингу персоналізовані електронні листи надсилають конкретній особі. Перед відправленням такого електронного листа зловмисник вивчає інтереси потенційної жертви. Наприклад, зловмисник дізнався, що ця особа цікавиться автомобілями і хоче придбати конкретну модель. Зловмисник приєднується до того ж обговорення на автомобільному форумі, що і жертва, готує фальшиву пропозицію продажу автомобіля і надсилає її жертві електронною поштою. Електронний лист містить посилання на фотографії автомобіля. Коли жертва переходить за посиланням, вона несвідомо встановлює зловмисне ПЗ на свій комп'ютер. Голосовий фішинг - це фішинг за допомогою технологій голосових комунікацій. Злочинці можуть робити фальшиві дзвінки, представляючись довіреними організаціями, за допомогою технології передачі голосу через IP. Жертви також можуть отримати записане повідомлення, яке виглядає легітимним. Таким чином злочинці намагаються отримати номери кредитних карток або іншу інформацію, щоб викрасти персональні дані жертви. Успішність голосового фішингу пояснюється довірою людей до телефонної мережі.

СМС фішинг– це вид фішингу, який використовує текстові повідомлення на мобільних телефонах. Злочинці видають себе за офіційне джерело щоб завоювати довіру жертви. Наприклад, під час СМС фішингу зловмисник може надіслати жертві посилання на веб-сайт. Коли жертва відвідає цей веб-сайт, на мобільний телефон буде встановлене зловмисне ПЗ. Фармінг - це фальшивий веб-сайт, що має вигляд справжнього, щоб змусити користувачів вводити свої облікові дані. Під час фармінгу користувачів спрямовують на фальшивий веб-сайт, який імітує офіційний. Потім жертви вводять свою особисту інформацію, вважаючи, що вони підключені до легітимного сайту. Whaling - це фішингова атака, що спрямована на осіб, які мають повний доступ до інформації в межах організації, наприклад, її вище керівництво. Також цілями можуть бути політики або знаменитості.

Зловмисники заражують веб-браузери з метою їх використання для відображення спливаючої реклами, збору особистої інформації або встановлення рекламного ПЗ, вірусів, шпигунських програм. Зловмисний код може бути встановлений у виконуваний файл браузера, компоненти браузера або його плагіни. Пошукові системи, такі як Google, ранжують веб-сторінки за результатами пошукових запитів користувачів. Положення веб-сайту в списку результатів пошуку залежить від релевантності його вмісту. SEO - це набір методів, що використовуються для підняття рейтингу веб-сайту у пошукових системах. Хоча багато легітимних компаній спеціалізуються на оптимізації веб-сайтів для покращення їх позиціонування, однак методи зловживання SEO використовують пошукову оптимізацію для того, щоб зловмисний веб-сайт піднявся в топ результатів пошуку. Найпоширенішою метою зловживання SEO є залучення відвідувачів на зловмисні веб-сайти, які можуть містити шкідливе ПЗ або використовувати соціальну інженерію. Щоб забезпечити зловмисному сайту вищу позицію в результатах пошуку, нападники використовують ключові слова з популярних пошукових запитів.

Викрадач браузерів - це зловмисне ПЗ, яке змінює налаштування веб-браузера на комп'ютері з метою перенаправлення користувача на проплачені веб-сайти. Викрадачі браузерів зазвичай встановлюються без дозволу користувача під час прихованого завантаження. Прихованим завантаженням називають програму, яка автоматично завантажується на комп'ютер, коли користувач відвідує певний веб-сайт або переглядає електронний лист в HTML. Завжди уважно читайте користувацькі угоди, коли завантажуєте програми, щоб уникнути загроз такого типу.

2.3 Рішення від зловмисного програмного забезпечення

Для захисту комп'ютеру від усіх видів зловмисного програмного забезпечення достатньо мати актуальне ПЗ та антивірусну програму. Більшість антивірусних пакетів успішно виявляють найпоширеніші форми шкідливого ПЗ. Проте щоденно кіберзлочинці розробляють і розповсюджують нові загрози. Тому ключем до ефективного захисту проти вірусів є постійне оновлення бази вірусних сигнатур. Сигнатура для віруса - це як відбиток пальця для людини. Вона ідентифікує характерні елементи зловмисного коду, за якими його можна розпізнати. Багато форм зловмисного ПЗ досягають своїх цілей через використання вразливостей програмного забезпечення як в операційних системах, так і в застосунках. Раніше вразливості операційної системи були основним джерелом проблем, на сьогоднішній день найбільший ризик становлять вразливості застосунків. В той час, як розробники операційних систем все швидше реагують на нові загрози, більшість розробників прикладного ПЗ на жаль нехтують цим.

Методи боротьби зі спамом включають фільтрування електронної пошти, навчання користувачів щодо обережного ставлення до підозрілих електронних листів та використання фільтрів на хостах/серверах. Важко

зупинити спам повністю, але можна зменшити його наслідки. Наприклад, більшість інтернет-провайдерів блокують спам, перш ніж він потрапить до поштової скриньки користувача. Більшість антивірусів та поштових клієнтів автоматично виконують фільтрацію електронних листів. Це означає, що вони виявляють та видаляють спам з електронної поштової скриньки користувача.

Організації також повинні попереджати працівників про небезпеку відкривання вкладень електронної пошти, які можуть містити віруси або Інтернет-черв'яки. Не вважайте, що вкладення електронної пошти є безпечними, навіть якщо вони надійшли від надійного джерела. Комп'ютер відправника може без його відому використовуватися для розповсюдження вируса. Завжди перевіряйте вкладення електронної пошти перед тим, як їх відкрити. Антифішингова робоча група - це галузева асоціація з протидії викраданню особистих даних та шахрайствам, які виникають в результаті фішингу або підробки електронних листів. Регулярне оновлення всього програмного забезпечення гарантує, що в системі є всі найновіші виправлення безпеки для усунення відомих вразливостей.

2.4 Загроза соціальною інженерією

Соціальна інженерія не використовує технічні засоби для збору інформації про майбутню жертву. Соціальна інженерія - це атака, під час якої злочинець намагається маніпулювати людиною, щоб змусити її до певних дій або до розголошення конфіденційної інформації. Соціальні інженери часто використовують бажання людей бути корисними, а також їх слабкості. Наприклад, зловмисник може подзвонити уповноваженому працівнику з приводу нагальної проблеми, вирішення якої вимагає негайного доступу до мережі. Зловмисник може розраховувати на марнославство співробітника, залякувати керівником або скористатися жадібностю працівника.

Є такі види атак соціальної інженерії, як претекстінг та послуга за послугу. Претекстінг - атакуючий телефонує конкретній особі і обманом намагається отримати доступ до привілейованих даних. Наприклад, зловмисник вимагає надати персональні або фінансові дані для підтвердження особи одержувача. Послуга за послугу - це коли злочинець запитує персональну інформацію в обмін на щось, наприклад, безкоштовний подарунок.

Соціальна інженерія спирається на декілька тактик. Повноваження - люди, як правило виконують дії, коли інструкції надходять з "авторитетного джерела". Залякування - злочинці змушують жертву до відповідних дій. Консенсус -люди вчинятимуть певні дії, якщо вони вважають, що інші зробили б так само. Дефіцит - люди діятимуть, якщо будуть думати, що кількість привабливих пропозицій обмежена. Терміновість - люди діятимуть, якщо вважатимуть, що мають обмежену кількість часу для прийняття рішення. Симпатія - злочинці будують приязні відносини з жертвою. Довіра - злочинці створюють довірчі відносини з жертвою, цей підхід може вимагати більше часу. Професіонали з кібербезпеки несуть відповідальність за ознайомлення інших співробітників організації з тактиками протистояння соціальній інженерії.

Уособлення - це спосіб видавати себе за когось іншого. Наприклад, нещодавня телефонна афера була спрямована на платників податків. Злочинець, який представлявся співробітником податкового управління, повідомляв жертвам, що вони мають заборгованість, яку жертви повинні сплатити негайно за допомогою банківського переказу. Самозванець погрожував, що відмова від сплати призведе до арешту. Злочинці також використовують уособлення, щоб атакувати інших. Вони можуть підірвати довіру до публічних осіб за допомогою публікацій на веб-сайтах або в соціальних мережах.

Містифікація або розіграш - це дія, призначена для обману. Містифікація в кібер-світі може завдати стільки ж клопоту, як і в реальному. Мета розіграшу - викликати реакцію жертви. Це може бути необгрунтований страх і нелогічна поведінка. Користувачі самі розповсюджують обмани через електронну пошту та соціальні мережі.

Несанкціоноване проникнення на територію відбувається тоді, коли зловмисник проникає до зони з обмеженим доступом слідом за уповноваженою особою. Для цього зловмисники використовують декілька способів. Він вдає ніби супроводжують уповноважену особу, приєднується до великої групи співробітників, вдаючи що також працюють в організації або вибирає жертву, яка легковажно ставиться до правил безпеки на об'єкті. Несанкціоноване проникнення слідом за зареєстрованим користувачем є ще одним терміном, який описує таку саму практику.

Запобігти несанкціонованому проникненню можна використовуючи тамбур-шлюзи з двома дверима. Після того, як співробітники входять у зовнішні двері, ці двері необхідно закрити перед тим як увійти у внутрішні двері.

Пересилання фейкових електронних листів з метою розіграшу, жартів, смішних фільмів, листів не пов'язаних із роботою, може порушити політику компанії з використання IT-інфраструктури та призвести до дисциплінарних покарань.

2.5 Рішення для захисту від соціальної інженерії

Організаціям необхідно підвищувати рівень поінформованості працівників про тактики соціальної інженерії та навчити працівників запобіжним заходам. Ніколи не надавати конфіденційну інформацію або

облікові дані невідомим особам електронною поштою, в чаті, особисто або телефоном. Не натискати на привабливі посилання в поштових повідомленнях та на веб-сайтах. Звертати увагу на несанкціоновані або автоматичні завантаження. Запровадити політику безпеки та ознайомити з нею працівників. Працівники повинні відчувати свою відповідальність за рівень безпеки в організації та не піддаватися тиску зі сторони невідомих осіб.

2.6 Огляд кібератак

Атака типу "Відмова в обслуговуванні" - є різновидом мережної атаки. Результатом DoS-атаки є переривання доступу користувачів, пристроїв або застосунків до мережних сервісів. Існує два основних типи DoS-атак перевантаження великою кількістю трафіку та пакети неправильного формату. При першому типі нападник надсилає величезну кількість даних з такою швидкістю, що мережа, хост або застосунок не встигає їх обробляти. Це спричиняє уповільнення передачі або реагування, іноді призводить до аварійного завершення роботи пристрою чи сервісу. Другий тип пердбачає що нападник надсилає пакет даних неправильного формату хосту або застосунку і одержувач не може його обробити. Наприклад, програма не може ідентифікувати пакети, що містять помилки або неналежним чином відформатовані. Це призводить до того, що приймаючий пристрій буде працювати дуже повільно або припинить роботу взагалі.

DoS-атаки несуть в собі велику небезпек, вони можуть порушувати коректну роботу системи, через це переривається обмін інформацією, а також в результаті таких атак втрачається багато часу та грошей. Їх особливістю є не складне проведення будь-яким користувачем мережі. Її метою є

неможливість доступу для всіх користувачів, які були авторизовані в атакованій мережевій інфраструктурі.

Досконалішою є розподілена DoS атака (DDoS), яка має подібні риси зі звичайною DoS, але проходить з декількох джерел. Якщо розглядати основний сценарій, то проходить таким чином: Злочинець заражає комп’ютери та під’єднує іх до своєї мережі, яка має назву ботнет, а комп’ютери, які в неї входять називаються зомбі. Комп’ютери-зомбі – це хости до яких зловмисник має доступ. Щоб мати контроль над хостами зловмиснки використовує керуючу систему. Зомбі сканують мережу та заражають знайдены в мережы комп’ютери, тим самим створюючи нових зомбі. Після сканування зловмисник може через керуючу систему розпочати DDoS атаку. Стуктурна схема DDoS атаки зображена на рисунку 2.2.

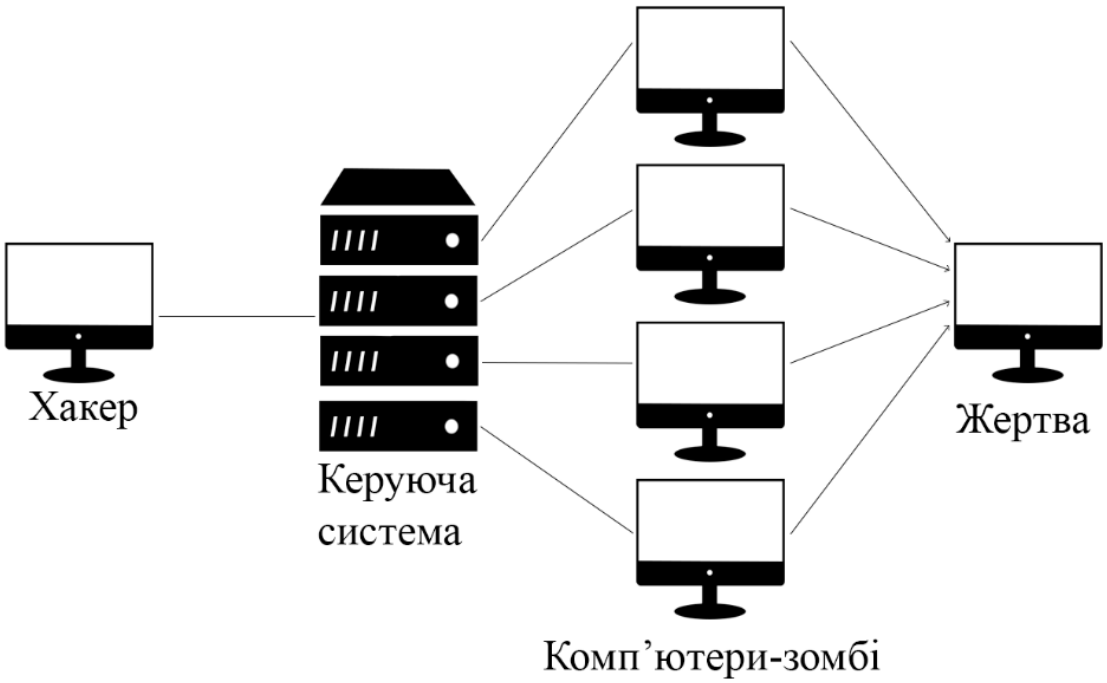

Рис 2.2 – Схема DDoS атаки

Sniffing є дуже схожим на підглядання за людиною в реальному світі. Хакери досліджують весь мережний трафік, який проходить через їх мережну інтерфейсну карту, незалежно від того, кому він адресований. Злочинці виконують аналіз трафіку в мережі за допомогою програмного

забезпечення, апаратного пристрою або їх комбінації. Sniffing переглядає весь мережний трафік або виконується фільтрація за певним протоколом, сервісом чи навіть за рядком символів, таких як ідентифікатор користувача або пароль. Деякі мережні аналізатори можуть перевіряти весь трафік і навіть змінювати його частково або повністю. Sniffing може бути корисним. Мережні адміністратори можуть використовувати такі засоби для аналізу мережного трафіку, визначення проблем з пропускною здатністю та вирішення інших проблем в мережній інфраструктурі. Фізична безпека має важливе значення для запобігання встановленню аналізаторів трафіку у внутрішній мережі організації.

Підміна являє собою атаку через встановлення довірчих відносин між двома системами. Коли ці системи синхронізуютсья і мають єдину аутентифікацію, користувач, увійшовши до однієї системи може повторно не аутинтефікуватися для отримання доступу до іншої. Це може стати і слабкістю системи, якою зловмисник неодмінно скористується. Він може відправити пакети до однієї з систем, який ця система сприймає як, надійшовший з система з довірчими відносинами. Цей пакет не проходить повторну аутентифікацію, так як між системами діють довірчі відносини, і зловмисники може надилати будь-які запити. Графічне зображення підміни можна побачити на рисунку 2.3.

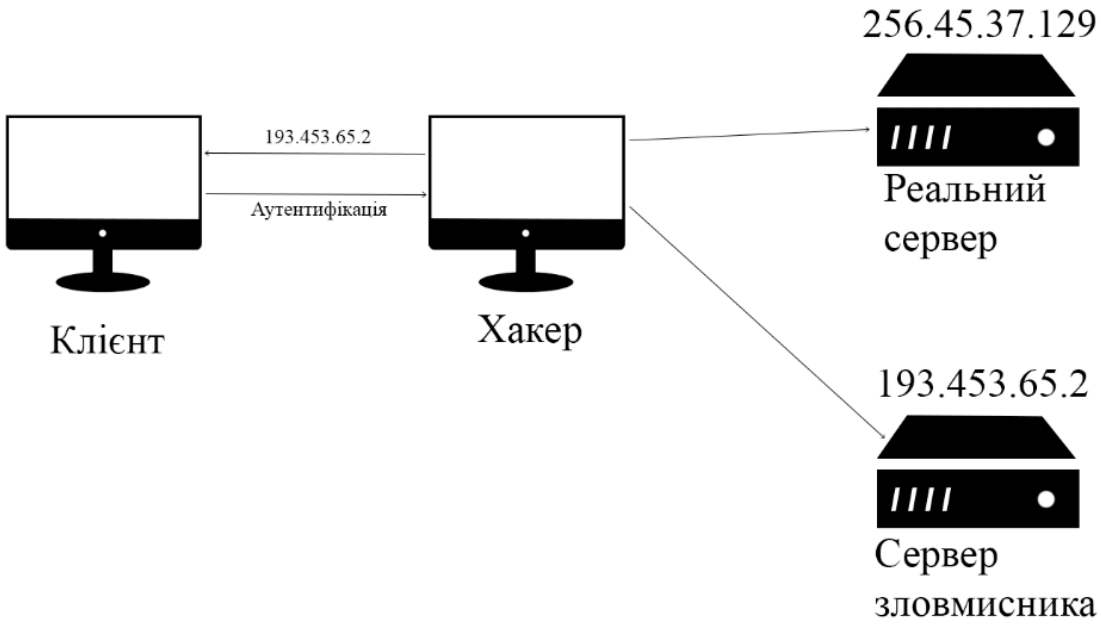

Рис 2.3 – Схема атаки типу підміна

Існує кілька типів атак з використанням підміни. Підміна MAC-адреси відбувається, коли один комп'ютер приймає пакети даних, адресовані на MAC-адресу іншого комп'ютера. IP-spoofing надсилає IP-пакети з підробленої IP-адреси джерела, щоб замаскувати свою справжню адресу. Протокол визначення адрес - це протокол, який перетворює IP-адреси в MAC-адреси для передачі даних. При ARP підміні зловмисник розсилає підроблені ARP повідомлення локальною мережею для того, щоб зв'язати свою MAC-адресу з IP-адресою авторизованого користувача мережі. Система доменних імен асоціює доменні імена з IP-адресами. При підміні DNS відбувається модифікація DNS-сервера для перенаправлення певного доменного імені на іншу IP-адресу, контрольовану злочинцем.

Злочинець, який виконує атаку Man-in-the-middle, перехоплює повідомлення, якими обмінюються комп'ютери, щоб викрасти інформацію, яка проходить мережею. Злочинець також може маніпулювати повідомленнями та передавати підставні дані між хостами, оскільки вузли не усвідомлюють, що відбулася модифікація повідомлень. MitM дозволяє злочинцю контролювати пристрій без відому користувача.

Man-In-The-Mobile - різновид атаки "Man-in-the-middle ". При MitMo зловмисник отримує контроль над мобільним пристроєм. Заражений мобільний пристрій пересилає конфіденційну інформацію користувача нападникам. ZeuS є прикладом експлойта з можливостями MitMo, який дозволяє атакуючим непомітно перехоплювати SMS-повідомлення 2-етапної авторизації, які надходять користувачам. Наприклад, коли користувач створює обліковий запис Apple, він повинен надати телефонний номер для отримання SMS з тимчасовим кодом підтвердження. Зловмисне ПЗ відстежує ці повідомлення та передає інформацію злочинцям. При реалізації атаки з повтором зловмисник перехоплює частину даних, які пересилаються між двома хостами, а потім повторно передає записане повідомлення. Такий спосіб дозволяє обійти механізми аутентифікації.

Атака нульового дня, яку іноді називають загрозою нульового дня, - це комп'ютерна атака, яка намагається використати вразливості ПЗ, що досі невідомі постачальнику програмного забезпечення, або які він приховує. Термін нульова година описує момент, коли хтось виявляє експлойт - шкідливий програмний код. Впродовж часу, доки виробник програмного забезпечення розробляє та випускає виправлення, мережа залишається вразливою для цього експлойту. Для захисту від цих стрімких атак професіоналам з мережної безпеки необхідно більш ретельно продумати архітектуру мережі. В наш час стримувати декілька вторгнень до системи одночасно у різних точках майже не можливо.

Клавіатурний шпигун - це програма, яка записує або вносить в спеціальний журнал натискання клавіш користувачем системи. Злочинці можуть реалізовувати кейлогери за допомогою ПЗ, встановленого на комп'ютері або через обладнання, фізично приєднане до комп'ютера. Зловмисник налаштовує ПЗ клавіатурного шпигуна таким чином, щоб воно відправляло зібрану в журналі інформацію електронною поштою. Перехоплені та записані до лог-файлу натискання клавіш можуть розкрити

імена користувачів, паролі, відвідані веб-сайти та іншу конфіденційну інформацію. Клавіатурні шпигуни можуть бути легальними, комерційними програмами. Батьки часто купують таке програмне забезпечення для відстеження поведінки дітей в Інтернеті та з'ясування того, які веб-сайти вони відвідують. Більшість анти-шпигунських програм здатні виявити та видалити несанкціоновані кейлогери. Хоча кейлогери не є незаконними програмами, але злочинці використовують їх для досягнення своїх незаконних цілей.

2.7 Рішення щодо захисту від атак

Організація може запровадити низку заходів для захисту від різноманітних атак. Налаштуйте міжмережні екрани так, щоб відхиляти будь-які пакети, що надходять ззовні мережі, але мають адреси, які вказують на їх походження з внутрішньої мережі. Така ситуація є незвичайною, і це вказує на те, що кібер-злочинець спробував здійснити атаку з підміною адреси.

Щоб запобігти DoS та DDoS атакам, переконайтеся, що патчі та оновлення є актуальними, розподіляйте навантаження між серверними системами та блокуйте зовнішні ICMP пакети на межі периметру. Мережні пристрої використовують ICMP-пакети для надсилання повідомлень про помилки. Наприклад, команда ping використовує ICMP пакети для перевірки чи може пристрій взаємодіяти з іншими пристроями в мережній інфраструктурі. Системи можуть попередити повторні напади, шифруючи трафік, використовуючи криптографічну аутентифікацію та включаючи часові мітки до кожної частини повідомлення.

2.8 Атаки на бездротові мережі та мобільні пристрої

З ростом популярності смартфонів умовно шкідливе ПЗ стає проблемою для безпеки мобільного доступу. Умовно шкідливе ПЗ включає дратівливі або небажані застосунки. Такі застосунки можуть не містити шкідливого ПЗ, але все одно становлять ризик для користувача. Наприклад, Grayware може відстежувати місцезнаходження користувача. Автори умовно шкідливого ПЗ зазвичай підтримують видимість легітимності, включивши опис функцій програми маленьким шрифтом до ліцензійної угоди. Користувачі встановлюють багато мобільних додатків, не ознайомлюючись з їх функціями.

Смішінг - коротка форма терміну SMS фішинг. Він використовує службу SMS для надсилання підроблених текстових повідомлень. Злочинці обманним шляхом змушують користувача відвідати веб-сайт або зателефонувати за номером телефону. Довірливі жертви можуть надавати таку конфіденційну інформацію, як інформація про кредитні картки. Відвідування веб-сайту може призвести до несвідомого завантаження користувачем шкідливого ПЗ, яке заразить його пристрій.

Несанкціонована точка доступу - це точка доступу, встановлена в захищеній мережній інфраструктурі без дозволу. Несанкціонована точка доступу може бути налаштована двома способами. Перший спосіб - працівник, керуючись добрими намірами, хоче спростити підключення мобільних пристроїв. Другий спосіб полягає в тому, що злочинці непомітно отримують фізичний доступ на територію організації і встановлюють несанкціоновану точку доступу. Оскільки обидва способи є несанкціонованими, вони становлять ризики для організації. Несанкціонована точка доступу також може означати точку доступу, яка використовується в злочинних цілях. У цьому випадку злочинці

налаштовують точку доступу для атак через посередника (MitM), щоб перехоплювати реєстраційні дані користувачів.

Для атаки типу "злий близнюк" використовується несанкціонована точка доступу з потужним сигналом і високою пропускною здатністю, щоб привабити користувачів. Після того, як користувачі підключаються до цієї точки доступу, злочинці можуть аналізувати трафік та виконувати MitM атаки.

Бездротові сигнали чутливі до електромагнітних та радіочастотних перешкод, а також до розряду блискавки або завад від флуоресцентних ламп. Бездротові сигнали також чутливі до навмисного глушіння. Радіочастотні перешкоди блокують сигнал радіо або супутникової станції, щоб він не доходив до станції отримувача. Частота, модуляція та потужність радіочастотних завад мають відповідати характеристикам пристрою, роботу якого хоче порушити злочинець.

Bluetooth - малопотужний протокол ближньої дії. Він використовується для передачі даних в персональній мережі, яка може містити такі пристрої, як мобільні телефони, ноутбуки та принтери. Є кілька версій Bluetooth. Він характеризується легким налаштуванням без необхідності використання мережних адрес. Bluetooth використовує спряження пристроїв для встановлення зв'язку між ними. Після встановлення синхронізації обидва пристрої використовують один і той самий ключ доступу.

Про вразливості Bluetooth давно відомо, але через обмежену зону дії протоколу, жертва та зловмисник повинні знаходитися близько один від одного. Bluejacking - це термін, який означає передачу несанкціонованих повідомлень на інший пристрій через Bluetooth. Як варіант цей спосіб використовують для розсилання шокуючих зображень. Bluesnarfing – це термін, що описує ситуацію, коли зловмисник копіює інформацію жертви з її

пристрою. Ця інформація може містити електронні листи та списки контактів.

Протокол безпеки, аналогічний захисту дротової мережі - це протокол безпеки, у якому розробники намагалися забезпечити в бездротових локальних мережах такий самий рівень безпеки, як в дротовій локальній мережі. Для захисту дротової локальної мережі застосовують заходи фізичної безпеки. Щоб забезпечити аналогічний захист даних, які передаються бездротовою локальною мережею, у WEP застосовують шифрування. WEP використовує ключ для шифрування. Керування ключами у WEP не передбачено, тому кількість людей, яким відомий один і той самий ключ, буде постійно зростати. Оскільки всі використовують один і той самий ключ, злочинець отримує доступ до великого обсягу трафіку для виконання аналітичних атак.

Захищений Wi-Fi доступ, а потім WPA2 замінили стандарт WEP через його слабкі місця. WPA2 не має таких проблем із шифруванням, оскільки зловмисник не може відновити ключ, аналізуючи трафік. Протокол WPA2 чутливий до атак, у яких кібер-злочинці можуть аналізувати пакети, що передаються між точкою доступу та легітимним користувачем. Кібер-злочинці використовують аналізатори пакетів, а потім запускають атаки в автономному режимі для підбору парольної фрази.

2.9 Захист від атак на бездротові мережі та мобільні пристрої

Для захисту від атак на бездротові мережі та мобільні пристрої необхідно зробити кілька кроків. Більшість WLAN пристроїв використовують налаштування за замовчуванням. Можна скористатися перевагами базових функцій безпеки бездротового зв'язку, такими як аутентифікація та шифрування, змінивши параметри конфігурації за

замовчуванням. Обмежити розташування точок доступу в мережній інфраструктурі, розмістивши ці пристрої за межами міжмережного екрану або у демілітаризованій зоні, яка містить інші недовірені пристрої, такі як поштові та веб-сервери.

WLAN утиліти, такі як NetStumbler, можуть виявляти несанкціоновані точки доступу або робочі станції. Розробляється політика гостьового доступу для вирішення задач підключення легітимних користувачів з правами гостя до Інтернету під час візиту до організації. Для віддаленого доступу авторизованих співробітників до WLAN використовуйте віртуальну приватну мережу. Інтерфейс утиліти NetStumbler зображено на рисунку 2.4.

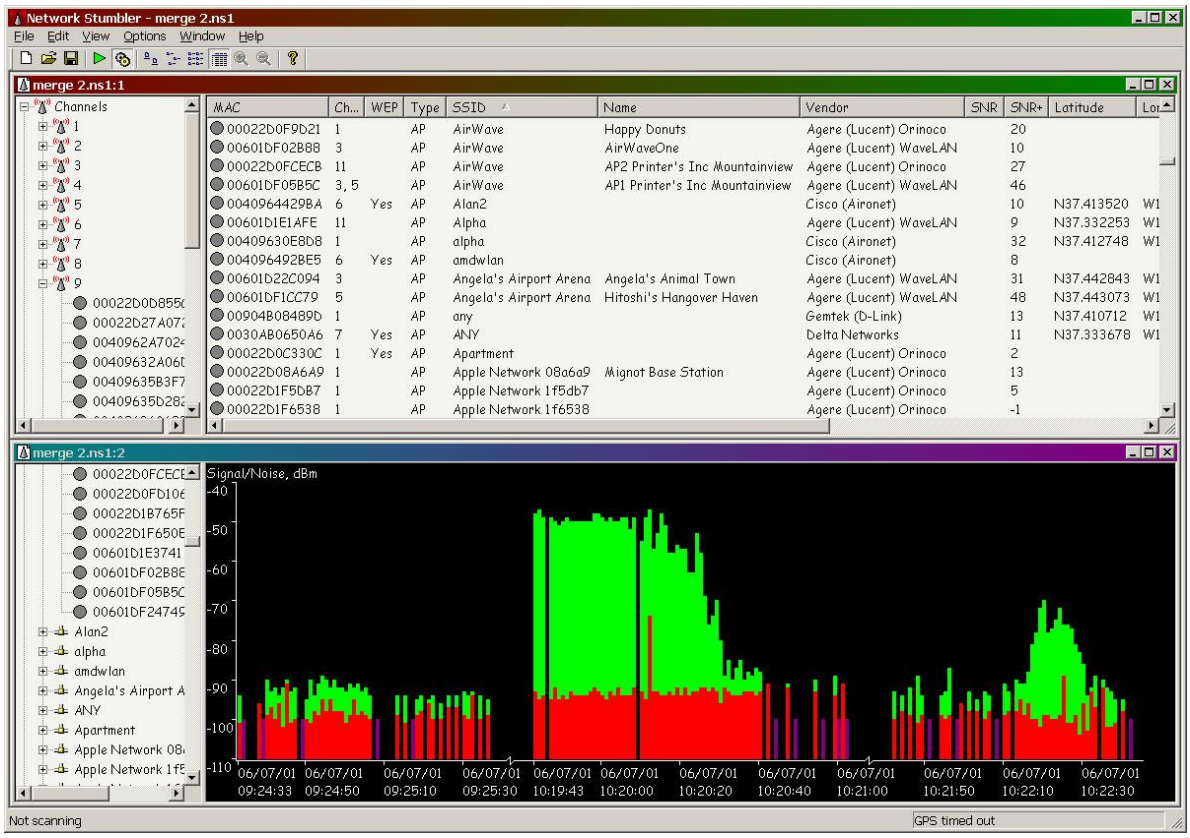

Рис 2.4 – Інтерфейс утиліти NetStumbler

2.10 Огляд атак на застосунки

Міжсайтовий скриптинг - вразливість, виявлена у веб-застосунках. XSS дозволяє злочинцям вбудовувати скрипти у веб-сторінки, які переглядають користувачі. Такий скрипт може містити зловмисний код. Міжсайтовий скриптинг включає трьох учасників: злочинець, жертва та веб-сайт. Кіберзлочинець не націлений на жертву напряму. Він використовує вразливість веб-сайту або веб-застосунку. Зловмисники вбудовують клієнтські скрипти до веб-сторінок, які переглядають користувачі-жертви. Шкідливий скрипт передається у браузер користувача без його відому. Шкідливий сценарій такого типу може мати доступ до будь-яких файлів cookie, ідентифікаторів сеансів або іншої конфіденційної інформації. Якщо злочинці отримують cookie-файл сеансу жертви, вони можуть видавати себе за неї.

Одним зі способів зберігання даних веб-сайту є використання бази даних. Існує декілька різних типів баз даних, такі як Structured Query Language база даних або Extensible Markup Language база даних. Напади з використанням XML та SQL ін'єкцій використовують недоліки в програмі, такі як неправильна перевірка запитів до бази даних.

При використанні XML у якості бази даних, XML-ін'єкція є атакою, яка може пошкодити дані. Після того, як користувач надає вхідні дані, система відправляє запит для отримання доступу до необхідної інформації в базі даних. Проблема виникає, коли система не належним чином перевіряє вхідний запит користувача. Злочинці можуть маніпулювати запитами, змінюючи їх відповідно до своїх потреб і отримати доступ до інформації в базі даних. Отримавши доступ до конфіденційних даних, що зберігаються в базі, зловмисники можуть внести будь-які зміни на веб-сайт. Атака XML-ін'єкції загрожує безпеці веб-сайту.

Кіберзлочинці використовують вразливості системи, вставляючи шкідливі SQL вирази у поля форм вводу. Як і в попередньому прикладі, система не фільтрує правильність введених користувачем символів в SQL - операторі. Злочинці використовують SQL ін'єкцію на веб-сайтах або в будь-якій SQL базі даних. Таким чином зловмисники можуть здійснити підміну ідентифікаційних даних користувачів, змінювати або знищувати існуючі дані в базі або стають адміністраторами сервера.

Переповнення буфера - відбувається, коли об'єм даних перевищує розмір виділеного буфера. Буфери - це області пам'яті, виділені для застосунку. Змінюючи дані за межами буфера, програма звертається до пам'яті, яка була виділена для інших процесів. Це може спричинити крах системи, призвести до несанкціонованого доступу до даних або ескалації прав користувача.

За оцінками спеціалістів координаційного центру CERT університету Карнегі-Меллона, майже половина вразливостей комп'ютерних програм так чи інакше обумовлені переповненням буферу. Існує велика кількість варіантів переповнення буфера, таких як: переповнення статичного буфера, помилки індексування, помилки форматування рядків, помилки в форматі рядка, невідповідність розмірів буферів Unicode і ANSI та переповнення динамічної області пам'яті.

Вразливості дозволяють кіберзлочинцям виконати зловмисний код і отримати контроль над системою з привілеями користувача, який запустив застосунок. Віддалене виконання коду дозволяє злочинцю виконати на цільовій машині будь-яку команду.

Metasploit - це інструмент для розробки та виконання зловмисного коду на віддаленому об'єкті. Meterpreter - це модуль Metasploit, який надає розширену функціональність. Meterpreter дозволяє злочинцям писати свої власні розширення як спільний об'єкт. Злочинці вивантажують і вбудовують

ці файли в процес, що запущений на машині жертви. Meterpreter завантажує та виконує всі розширення з пам'яті, тому вони ніколи не залучають ресурси жорсткого диску. Це також означає, що антивірусні програми не можуть їх виявити. Meterpreter має модуль для віддаленого керування веб-камерою. Як тільки злочинець встановлює Meterpreter в систему жертви, він може вести відеоспостереження та робити знімки з веб-камери на пристрої потерпілого.

2.11 Захист від атак на застосунки

Перша лінія захисту від атак на застосунки полягає у написанні надійного коду. Незалежно від того, яка мова програмування та джерело вводу інформації використовуються, доцільно розглядати всі вхідні дані як потенційно ворожі. Потрібно перевіряти всі вхідні дані так, ніби вони є потенційною загрозою.

Все програмне забезпечення, включно з операційними системами та прикладними програмами, має бути оновленими і не можна ігнорувати повідомленя про оновлення. Не всі програми оновлюються автоматично.

3 МЕТОД БОРОТЬБИ З АТАКАМИ ДОСТУПУ В СУЧАСНИХ МЕРЕЖАХ

3.1 Аналіз технології Fail2ban

Fail2ban[4] являє собою програмне забезпечення, яке усуває можливість несанкційованого доступу, воно захищає комп'ютер від атак грубої сили. Ця технологія написана на мові програмування Python працювати в системах POSIX, таких як ip-таблиці або tcp-оболонці, які мають мають інтерфейс керуючий системою управління пакетами або брандмауєра. Воно використовує регулярні вирази для сканування файлів журналу, пошук експлойтів. Найчастіше це використовується для блокування вибраних IP-адрес, які можуть належати вузлам, які намагаються порушити безпеку системи. Підраховуються всі записи, відповідні шаблонам, і коли їх кількість досягає певного зумовленого порогу, Fail2ban блокує IP-адресу порушника за допомогою системного брандмауера на певний період часу. Після закінчення терміну заборони IP-адреса видаляється з забороненого списку. Зазвичай Fail2ban використовується для оновлення правил брандмауєра. За замовченням в ньому встановлено фільтри для таких служб, як apache, ssh, courier.

Дана технологія підтримує роботу з IPv4 та IPv6. Вона також, запам'ятовувати користуввачів та при кількоразовому порушенні час блокування збільшується. Але для зупинення шкідливого мережевого з'єднання достатньо декількох хвилин блокування.

Стандартно Fail2ban містить два файли конфігурації jail.conf та defaults-debian.conf. Не рекомендується змінювати ці файли, так як вони можуть бути перезаписані при оновленні пакета. Вони являють собою основу захисту від шкідливого хосту, який намагаєтсья отримати доступ до певних мережевих служб. Найчастіше Fail2ban встановлюється з дистрибутива і налаштовується

по мануалам з інтернету. Потім роками працює без зовнішнього втручання адміністратора

3.2 Розробка методу захисту мережі від атак грубої сили за допомогою технології Fail2ban

Fail2ban на час встановлений адміністратором забороняє IP-адресі доступ до серверу. Якщо хтось з мережі не зможе згадати пароль за встановлену мережевим адміністратором кількість спроб, то всі люди в даному офісі втратять доступ до цього сервера. Але якщо сервер буде налаштований за допомогою власних сценаріїв Fail2ban, захист буде надійний при цьому доступ буде збережений для користувачів з будь-якою IP-адресою.

Якщо хакер спробує отримати доступ методами грубої сили, після невдалих спроб з поточної IP-адреси він може змінити її для перебору. Проти цього також допоможуть власні сценарії Fail2ban, які сильно сповільнюють дії хакера. Щоб уникнути згаданих проблем, скрипти блокують IP-адресу не на деякий час, а сповільнюють швидкість його з'єднання із сервером. Отже, хакер не може застосовувати грубий перебір 100 або 1000 разів на секунду, а лише, наприклад, 1 раз на секунду. В основній папці дій Fail2ban створено файл .conf з ім'ям slow-ban.conf. У цьому файлі буде викликатись скрипт, який показаний на рисунку 3.1. У цьому новому сценарії ми додамо правило iptables, яке обмежить вхідну швидкість для конкретної IP-адреси до 1 пакету в секунду, також це число можна змінити в slow-ban.conf.

```
[Definition]

actionstart = bash /etc/fail2ban/action.d/slow-ban-iptables.sh start

actionstop = bash /etc/fail2ban/action.d/slow-ban-iptables.sh stop

actioncheck =

actionban = bash /etc/fail2ban/action.d/slow-ban-iptables.sh ban <ip>

actionunban = bash /etc/fail2ban/action.d/slow-ban-iptables.sh unban <ip>

[Init]
```

Рис 3.1 – скрипт файлу slow-ban.conf

На рисунках 3.2 та 3.3 показано скрипт slow-ban-iptables.sh файлу, в якому задаються функції show_usage, яка виводить інформацію про дію над адресою та її IP, ban_ip, яка уповільнює хост на задану кількість часу, та unban_ip, яка знімає блокування.

```
#!/bin/bash

function show_usage {
    echo "Usage: $0 action <ip>"
    echo "Where action is start, stop, ban, unban"
    echo "and ip is optional passed to ban, unban"
}

speed=1

function ban_ip {
    iptables -A INPUT -p tcp -s $1 --dport 20 -m limit --limit $2/sec -m
state --state ESTABLISHED -j ACCEPT
    echo "Baned $1 with speed $2/sec" > /home/andrii/logs.log
    exit
}

function unban_ip {
    iptables -D INPUT -p tcp -s $1 --dport 20 -m limit --limit $2/sec -m
state --state ESTABLISHED -j ACCEPT
    echo "Unbaned $1" > /home/andrii/logs.log
    exit
}
```

Рис 3.2 - скрипт функцій файлу slow-ban-iptables.sh

```
if [ $# -lt 1 ]
then
    show_usage
fi

if [ "$1" = 'start' ]
then
    echo 'Fail2ban Slow Ban Started'
elif [ "$1" = 'stop' ]
then
    echo 'Fail2ban Slow Ban Stoped'
elif [ "$1" = 'ban' ]
then
    if [ $3 ]
    then
        speed=$3
    fi
        ip=$2
        ban_ip $ip $speed
elif [ "$1" = 'unban' ]
then
    ip=$2
    unban_ip $ip
else show_usage
fi
```

Рис 3.3 - скрипт умовних операторів файлу slow-ban-iptables.sh

Для застосування налаштування на підключення по протоколу ssh, як показано на рисунку 3.4. потрібно додати banaction = slow-ban, цей рядок повідомляє Fail2ban використовувати файл slow-ban.conf для обмеження з'єднань по ssh.

```
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and de>
#mode   = normal
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
banaction = slow-ban
```

Рис 3.4 – скрипт файлу Jail.local

3.3 Оцінка ефективності розробленого методу

Для оцінки ефективності цього методу достатньо розрахувати безпечний час використання пароля. Це час поки зловмисник виконує повний перебір паролів методом грубої сили. Щоб знайти безпечний час використання пароля *T*, потрібно кількість всіх можливих комбінацій *Q* помножити на час однієї спроби *Ts* (3.1):

$$T = Q * Ts \tag{3.1}$$

Якщо система захищена 6-значним паролем, без fail2ban slow-ban зі швидкістю методу грубої сили в 100 спроб в секунду час безпечного використання паролю буде рівним 850800 днів. А при застосуванні цієї технології швидкість перебору методом грубої сили не зможе перевищути 1 спроби в секунду, а кількість днів безпечного використання збульшується до 8508007. Як видно персональний скрипт збільшує час до повного перебору у стільки разів, наскільки швидше зловмисник перебирає пароль без блокування на 1 спробу в секунду.

Для більшої наглядності можна розглянути шанс паролю не бути знайденим *Pp* протягом певного періоду часу *t*, з використанням часу однієї спроби підбору пароля *T* та часу, що нас цікавить *t* (3.2):

$$Pp(t) = t * T \tag{3.2}$$

Для періоду часу в 20 днів в системі з 6-значним паролем шанс розкриття паролю буде рівним 0.0000235, але якщо система захищена Fail2ban slow-ban шанс дорівнюватиме 0.00000235. Як видно персональний скрипт зменшує шанс паролю бути розкритим у стільки разів, наскільки швидше зловмисник перебирає пароль без блокування на 1 спробу в секунду.

Таким чином, сценарій fail2ban для обмеження швидкості спроб brute force дозволяє підключитися до сервера за допомогою SSH, але не блокує весь трафік SSH. Таким чином, він захищає концепцію fail2ban від заборони дозволених користувачів, а також добре захищає сервер. Звичайно, заборона за замовчуванням буде більш безпечною. Але для деяких користувачів або серверів цей скрипт буде дуже корисним. Безпека сервера зростатиме в стільки разів, у скільки 1 пакет в секунду повільніший, ніж швидкість методу грубої сили хакера. Також існує ймовірність того, що протягом деякого

фіксованого часу пароль буде підібраний в цій роботі був розрахований час для двох випадків - без fail2ban та з персональним скриптом.

ВИСНОВОК

Актуальною і важливою темою в сучасному Інтернеті є тема інформаційної безпеки. На даний час існує велика кількість факторів, які загрожують користувачам і підприємствам в Інтернеті. Така кількість загроз зумовлена тим, що технології в Інтернеті розвиваються швидше ніж сфера захисту від них. Для протидії атакам потрібно, щоб вони спочатку з'явились. А аналіз атаки та знаходження методів для боротьби з ними може зайняти великої кількості часу.

В світі кібербезпеки можна спостерігати такі поняття, як загроза, що являє собою можливість, того що відбудеться небезпечна подія, яке може призвести до втрат, як вразливість, що представляє з себе ваду, що робить ціль вразливою до атаки, та як атака, що безпосередньо є навмисним використанням виявлених вразливостей комп'ютерних систем.

Для посиленого та гнучкого контролю над мережею створена концепція Fail2ban, яка блокує доступ користувачами, представляючим загрози. Вона полягає у відмові пакетам з певної IP–адреси зловминсника на певний час, і зловмисник з цієї IP–адреси більше не може отримати доступ до сервера. Fail2ban буде блокувати весь трафік користувачів, які перебувають позаду NAT мережі. Тобто якщо користувач позаду NAT буде заблокований, разом з ним будуть заблоковані всі інші користувачі. Але якщо сервер буде налаштований за розробленим методом, він все одно може бути дуже захищений, надавши доступ для дозволених користувачів з будь-якої IP-адреси. Для розуміння рівня захисту серверу після налаштування далі будуть розрахунки оцінки ефективності розробленого методу. Цей метод добре підходить для боротьби з атаками до доступу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Оліфер В. Г., Оліфер Н. А. Комп'ютерні мережі.
2. Бірюков А. А. Інформаційна безпека: захист і напад.
3. Юрій Діогенес, Ердаль Озкайя Кібербезпека стратегії атак і оборони.
4. Офіційний сайт fail2ban [Електронний ресурс] / Режим доступу: https://www.fail2ban.org/wiki/index.php/Main_Page