**\*Назва навчального закладу\***

**Факультет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

***Кафедра \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

**Реферат**

**з курсу**

**«Комп’ютерні мережі»**

## ТЕМА: хмарні технології

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Група \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Викладач: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Київ 2023**

Зміст

[ТЕМА: Поширені види мережевих атак і способи захисту від них 1](#_Toc154002091)

[Вступ 3](#_Toc154002092)

[Типи і приклади мережевих атак 3](#_Toc154002093)

[Визначити DDoS атаку 11](#_Toc154002094)

[Висновок 12](#_Toc154002095)

[Список використаних джерел 12](#_Toc154002096)

# Вступ

**В сучасному цифровому світі, де мережі пронизують у всі сфери нашого життя, питання кібербезпеки стають надзвичайно важливими. Ми живемо в епоху, коли інтернет та комп'ютерні технології визначають розвиток суспільства, економіки та науки. Однак разом із зростанням обсягів інформації та комунікацій збільшується і загроза мережевих атак.**

Важливо розуміти, що кібербезпека – це постійний процес, який вимагає не лише технічних засобів, але і уваги до людського фактору та вдосконалення стратегій захисту відповідно до зростаючих загроз. Тільки комплексний підхід до кібербезпеки дозволяє стежити за розвитком загроз та ефективно захищати мережеві ресурси в сучасному цифровому середовищі.

Типи і приклади мережевих атак

Мережеві атаки поділяють на **активні** і **пасивні**.

**Активні атаки** включають у себе явний вплив на систему, який змінює її стан. Наприклад, це може бути шкідливий програмний код-вірус, впроваджений в виконувану системою програму, спотворення даних на сторінках веб-сайту, блокування мережевого сервісу шляхом "бомбардування" його помилковими запитами. Відмінністю активних атак є те, що після свого завершення вони, як правило, залишають сліди.
Наприклад, змінюється вміст пам'яті, надходять дивні діагностичні повідомлення, додатки починають виконуватися неправильно, уповільнено або взагалі зависають, в характеристиках мережевого трафіку і в інших статистичних даних про роботу системи з'являються незрозумілі сплески активності. Проте ретельно підготована ​​активна атака може пройти непоміченою, якщо фахівці, що відповідають за її безпеку, погано інформовані про можливі наслідки такого роду атак.

**Пасивні атаки** не порушують нормальну роботу системи: вони пов'язані зі збором інфорції про систему, наприклад, вони можуть прослуховувати внутрішньомережевий трафік або перехоплювати повідомлення, передані по лініям зв'язку. У багатьох випадках пасивні атаки не залишають слідів, тому їх дуже складно виявити, часто вони так і проходять непоміченими.

На практиці рідко зустрічається активна або пасивна атакою «в чистому вигляді». Найчастіше атака включає підготовчий етап - етап збору інформації про цільову систему,  а потім на основі зібраних даних здійснюється активне втручання в її роботу. До корисної для хакера інформації відносяться типи ОС і додатків, IP-адреси, номера портів, імена і паролі користувачів.

Відмова в обслуговуванні
До числа активних атак відносяться дві вельми поширені атаки: **відмова в обслуговуванні** і **розподілена атака відмови в обслуговуванні**.В першому випадку, система, призначена для виконання запитів легальних користувачів, раптом перестає це робити або робить з великими затримками, що еквівалентно відмові. Відмова в обслуговуванні може трапитися у разі зловмисних дій, коли перевантаження створюється спеціально: на комп'ютер, що піддається атаці, надсилається інтенсивний потік запитів, згенерованих засобами атакуючого комп'ютера. Цей потік «затоплює» атакований комп'ютер, викликаючи в нього перевантаження, і в кінцевому етапі робить його недоступним. Блокування відбувається в результаті вичерпання ресурсів процесора, або операційної системи, або каналу зв'язку (смуги пропускання).

Зловмисник може багаторазово посилити ефект від проведення атаки відмови обслування шляхом крадіжки чужої обчислювальної потужності задля власни потреб. Для цього він отримує контроль над атакованим комп'ютером, завантажує в нього спеціальне шкідливе програмне забезпечення і активує його. Таким чином зловмисник непомітно для власника, "відгалужуючи" частину його обчислювальної потужності, змушуює інший комп'ютер працювати на себе.

|  |
| --- |
| https://1.bp.blogspot.com/-KZNjqykfbmw/Wiuws0jKCJI/AAAAAAAABas/tNcrFNEqgwwR5mw9MeN6phLVoUrOB1ZcACLcBGAs/s640/ddosattackwork.jpg |

При цьому власникові комп'ютера не завдається ніякої іншої шкоди, крім зниження продуктивності його комп'ютера. Для проведення потужної атаки зловмисник захоплює контроль над деякою кількістю комп'ютерів, організовує їх узгоджену роботу і направляє весь сумарний потік запитів з цих комп'ютерів на комп'ютер-жертву. Кажуть, що в таких випадках має місце **розподілена атака відмови в обслуговуванні** (Distributed Denial of Service, DDoS), або DDoS-атака.

Спуфінг

При проведенні атак зловмисникові важливо не тільки досягти своєї мети, яка полягає в заподіянні шкоди атакованому об'єкту, але і знищити всі сліди своєї
діяльності. Одним з основних прийомів, використовуваних зловмисниками для "замітання слідів", є **підміна вмісту пакетів**, або**спуфінг** (spoofing). Зокрема, для приховування місця знаходження джерела шкідливих пакетів зловмисник змінює значення поля адреси відправника в заголовках пакетів. Оскільки адреса відправника генерується автоматично системним програмним забезпеченням, зловмисник вносить зміни в відповідні програмні модулі так, щоб вони давали йому можливість відправляти  зі свого комп'ютера пакети з будь-якими IP-адресами.

|  |
| --- |
| https://4.bp.blogspot.com/-sbYKSe3I-rE/Wiu1bUo_a1I/AAAAAAAABaw/8Pr24tJzDtc3E5ThIq3c2VoVw-cTfelhgCLcBGAs/s400/1200px-IP_spoofing_en.svg.png |
| Приклад спуфінгу |

Ще важче визначити адресу джерела розподіленої атаки, так як безпосередніми виконавцями виступають "зомбовані" комп'ютери і саме їх адреси містяться в полі адреси відправника пакетів. І хоча нічого не підозрюючі власники комп'ютерів-виконавців стають учасниками розподіленої атаки проти своєї волі, велика частина відповідальності лягає і на них. Адже саме їх прогалини в забезпеченні безпеки власних систем зробили ​​цю атаку можливою.

Впровадження шкідливих програм
Численна група активних атак пов'язана з впровадженням в комп'ютери шкідливих програм (malware - скорочення від malicious software). До цього типу програм відносяться троянські та шпигунські програми, руткіти, черв'яки, віруси, спам, логічні бомби і ін. Ці програми можуть проникати на атаковані комп'ютери різними шляхами. Найпростіший з них - "самодоставка", коли користувач самостійно завантажує файли з неперевірених джерел або безтурботно відкриває підозрілий файл, який прийшов до нього як додаток по електронній пошті. Існують і більш складні представники шкідливих програм, що володіють власними механізмами "розмноження": копії таких програм поширюються по комп'ютерній мережі без участі користувачів.

|  |
| --- |
| https://3.bp.blogspot.com/-Mr8rapxipuM/Wiu3pIW6IzI/AAAAAAAABa0/oTWvrxkrbbsTAQUwTxu2aocZMSLxNpYYACLcBGAs/s640/cc4cd94ba51046de97252d312389fb6e.jpg |
| Приклад впровадження шкідливої програми Liberpy  |

Одним із прикладів шкідливих програм є шпигунські програми (spyware), які таємно (як правило, віддалено) встановлюються зловмисниками на комп'ютери нічого не підозрюючих користувачів, щоб відстежувати і фіксувати всі їхні дії. Зібрана інформація пересилається зловмисникові, який застосовує її в злочинних цілях.

Фішинг

**Фішинг** (phishing - спотворене fishing) використовується шахраями, що видають себе за довірених осіб, для "вивудження" персональних даних, наприклад логінів і паролів. Це може досягатися шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень всередині різних сервісів. У листі може міститись пряме посилання на сайт, який ззовні не відрізнити від справжнього, або на сайт з перенаправленням.
Також проявами фішингу можуть бути спливаючі вікна, що з'являються на сайтах, яким ми цілком та повністю довіряємо і майже без роздумів можемо довіритись цьому вікну, яке навіть стилістично оформлено під сайт.
Сніфери **пакетів**

Сніффер пакетів являє собою прикладну програму, яка використовує мережеву карту, що працює в режимі promiscuous mode (у цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатку для обробки). При цьому сніффер перехоплює усі мережні пакети, які передаються через певний домен.

|  |
| --- |
| https://4.bp.blogspot.com/-2ZnbfYS7hPs/Wiu5r_V_8-I/AAAAAAAABa4/WF-CJJt8aJsqGtfZ7MlEIcPgzrBvDGXhACLcBGAs/s320/simple.png |
| Простий приклад сніфінгу, у якому всі повідомлення (пакети) між абонентами відстежуються |

В даний час сніффери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і аналізу графіка. Однак з огляду на те, що деякі мережеві додатки передають дані в текстовому форматі (Telnet, FTP, SMTP, POP3 і т.д.), за допомогою сніффера можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі). Перехоплення імен і паролів створює велику небезпеку, тому що користувачі часто застосовують один і той же логін і пароль для безлічі додатків і систем.

Атаки Man-in-the-Middle

Для атаки типу Man-in-the-Middle хакеру потрібний доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від провайдера в будь-яку іншу мережу, може, приміром, отримати співробітник цього провайдера. Для атак цього типу часто використовуються сніффери пакетів, транспортні протоколи та протоколи маршрутизації. Атаки проводяться з метою крадіжки інформації, перехоплення поточної сесії і отримання доступу до приватних мережевих ресурсів, для аналізу трафіку та отримання інформації про мережу та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережеві сесії, Ефективно боротися з атаками типу Man-in-the-Middle можна тільки за допомогою криптографії. Якщо хакер перехопить дані зашифрованої сесії, у нього на екрані з'явиться не перехоплене повідомлення, а безглуздий набір символів. Зауважимо, що якщо хакер отримає інформацію про криптографічний сесії (наприклад, ключ сесії), це може зробити можливою атаку Man-in-the-Middle навіть в зашифрованому середовищі.

Способи виявлення мережевих атак

**Брандмауер** - це поєднання програмних та апаратних засобів, які ізолюють внутрішню мережу від Інтернету, пропускаючи одні пакети і блокуючи інші. Брандмауер дозволяє адміністратору мережі контролювати доступ до ресурсів корпоративної мережі, що здійснюється зовні, а також керувати ресурсами адміністрованої мережі , регулюючи вхідний та вихідний трафік.

Всі брандмауери можна поділити на три категорії: **традиційні пакети фільтрів**, **фільтри, що враховують стан з'єднання** та **шлюзи додатків**.

Традиційні фільтри пакетів

Весь вхідний та вихідний трафік внутрішньокорпоративної мережі проходить через маршрутизатор, на якому відбувається фільтрація пакетів. Фільтр пакетів перевіряє кожну дейтаграмму, визначаючи як що з нею зробити згідно з правилами, встановленими адміністратором мережі. Адміністратор мережі конфігурує брандмауер, спираючись на політику, що діє в організації.

|  |
| --- |
| https://3.bp.blogspot.com/-4H4wTzsdaRg/Wiu8HSoojbI/AAAAAAAABa8/Tv9R2yF9YeUq7jk9fqu7jDnX7IfiB65RgCLcBGAs/s400/bssl_0205.gif |
| Файрвол фільтрує пакети: якщо пакет відповідає вимогам, то він проходить, в іншому разі - ні |

Рішення , пов'язані з фільтрацією, зазвичай засновані на наступних факторах: вихідна чи кінцева ІР-адреса, тип протоколу в відповідному полі дейтаграми, флагові біти, тип повідомлення, різні правила, що характеризують вхідні і вихідні дейтаграми даної мережі та правила, що стосуються інтерфейсів.
Правила брандмауера реалізуються в маршрутизаторах за допомогою списків контролю доступу. Ці правила застосовуються для кожної дейтаграми, яка проодить через даний інтерфейс.

Фільтри, які враховують стан з'єднання

Дані фільтри відстежують ТСР-з'єднання і виконують фільтрацію на основі цієї інформації. Всі поточні ТСР-з'єднання відстежуються в спеціальній таблиці з'єднань. Якщо ж вхідний пакет не буде відноситись до поточних з'єднань, то він буде відкинутий брандмауером.

|  |
| --- |
|  |

Брандмауер має змогу фіксувати створення нового з'єднання, закінчення з'єднання, та перевірити активність з'єднання.

Шлюз **додатків**

Для забезпечення більш адресної безпеки, брандмаузери повинні комбінувати при роботі пакетні фільтри та шлюзи додатків. Шлюз додатків переглядає не лише загаловки, але й приймає рішення щоод дотримання політки на основі данного прикладного рівня. Шлюз додатків - це сервер, що працює на прикладному рівні, і через цей шлюз мають протікати всі дані додатків (вхідні і вихідні). На одному хості може працювати одразу декілька шлюзів додатків, проте кожний шдюз - це самостійний сервер з власним набором процесів.

|  |
| --- |
|  |

Для виявлення багатьох типів атак нам потрібно виконувати поглиблену перевірку пакетів - аналізувати не лише поля заголовків, а й дані додатків, що містяться у пакеті. Шлюзи додатків можуть виконувати дану операцію, проте вони вирішюють цю задачу лише для конкретного додатку.

Системи виявлення вторгнень
**Система виявлення вторгнень**дозволяє виявити різні атаки, а саме трасування мережі, сканування портів, стеків ТСР, атаки відмови в обслуговуванні, застосування червів та вірусів, атаки на вразливості операційної системи чи окремих додатків.
В мережі організації можуть бути декілька таких систем. При одночасній роботі вони працюють узгоджено , пересилаючи повідомлення про підозрілий трафік в центральний процесор системи, який збирає та систематизує ці дані, а також повідомляє адміністратору якщо це необхідно.

|  |
| --- |
|  |

Системи виявлення сигнатур можна розділити на дві категорії: ті, що працюють **на основі перевірки сигнатур** і ті, що працюють **на основі виявлення аномалій**.
Система, що працює **на основі перевірки сигнатур**, веде обширну базу даних сигнатур атак. Кожна сигнатура - це набір правил, що описують способи боротьби з вторгненнями. Дана система аналізує кожний пакет, що проходить повз неї, порівнюючи його вміст з сигнатурами бази данних. Якщо пакет співпадає з сигнатурою, то генерується попередження. Проте мінусом даного підходу є те, що система безсильна проти незареєстрованих атак, співпадіння сигнатур може бути зовсім не атакою, а також при порівнянні пакету з величезною колекцією сигнатур система може просто не впоратись з такою роботою і проґавити шкідливі пакети.

Система, що працює **на основі виявлення аномалій**, створює профіль надійного трафіку, який спостерігається у штатному режимі. Потім вона відстежує такі потоки пакетів, які мають, статичні дивацтва. Наприклад непропорціональне збільшення пакетів, чи різкий скачок інтенсивності сканування портів. Гарною стороною є те, що вони можуть відстежувати нові, ще не описані атаки, проте з іншої сторони, виключно важко розрізняти нормальній і статично незвичайний трафік.
Опис програми WideShark
Wireshark - продукт з відкритим вихыдним кодом, выльно поширюваний на підставі ліцензії GPL. Працює на більшості сучасних ОС (Microsoft Windows, Mac OS X, UNIX).
Перехоплює трафік мережевого інтерфейсу в режимі реального часу. Wireshark може перехоплювати трафік різних мережевих пристроїв, відображуючи його ім'я (включаючи безпровідні пристрої). Подтримка того або іншого пристрою залежить від багатьох чинників, наприклад від операційної системи.Підтримує множину протоколів (TELNET, FTP, POP, RLOGIN, ICQ, SMB, MySQL, HTTP, NNTP, Xll, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, MSN, YMSG і інші).
Збереження і відкриття раніше збереженого мережевого трафіку.Імпорт і експорт файлів з інших пакетних аналізаторів. Wireshark може зберігати перехоплені пакети у велику кількість форматів інших пакетних аналізаторів, наприклад: libpcap, tcpdump. Sun snoop, atmsnoop, Shomiti/Finisar Surveyor, Novell LANalyzer, Microsoft Network Monitor, AIX's iptrace.
Дозволяє фільтрувати пакети по множині критерій.
Дозволяє шукати пакети по множині критерій.
Дозволяє створювати різноманітну статистику.

Визначити DDoS атаку за допомогою програми можна таким способом. Можна відфільтрувати окремі адреси джерел пакетів (на малюнку це не зображено), та проаналізувати колонки Time та DestPort. Якщо значення DestPort співпадають, то це явна ознака DDoS атаки. Ознайомтеся також зі стовпцем Time. Зауважте, як мало часу між кожним пакетом - всього тисячі секунд. Це ще одина ознака атаки DoS.

|  |
| --- |
|  |
| При аналізі пакетів корисно також переглядати вкладку Flags. Там знаходиться прапор фрагментації. Цей прапор повідомляє одержуючій системі,чи пакет фрагментований чи ні. Зазвичай встановлено значення "Don't fragment", за винятком випадків, коли пакет фрагментований (тоді він встановлений на "More fragments"). У нашому випадку не встановлено жодного прапора. Це серйозна ознака шкідливого трафіку, оскільки для звичайного трафіку будь-який з цих прапорів буде встановлено, але ніколи не буде пустим.

|  |
| --- |
|  |

За допомогою фільтра arp.duplicate-address-frame можна відстежувати прояви спуфінгу. На малюнку зображено приклад, у якому різні ІР-адреси мають однакові МАС-адреси.Іноді також може бути корисним перегляд ТСР потоку певного потоку. Це можна зробити клацнувши правою кнопкою миші на пакеті та обрати TCP Stream.Наприклад, за допомогою цієї ж програми можна дізнаватись про дані такі як логіни та раполі. Для прикладу можна зайти на будь-який сайт та авторизуватись. Після цього перейти в програму та переглянути яку ми зумовили активність. За допомогою фільтру **http.request.method == “POST”**віднайдемо пакет з даними та відкриємо його ТСР потік. Після цього в новому вікні з'явиться текст, який в коді відновлює вміст сторінки. Знайдемо поля «password» і «user», які відповідають паролю та імені користувача. У деяких випадках обидва поля будуть легко читатися і навіть не зашифруватися, але якщо ми намагаємося захопити трафік при зверненні до дуже відомих ресурсів типу: Mail.ru, Facebook, Вконтакте тощо, то пароль буде закодований. ВисновокУ висновку можна підкреслити той факт, що зростання важливості мережевих технологій супроводжується збільшенням загроз кібербезпеці. Поширені види мережевих атак, такі як атаки на конфіденційність, цілісність та доступність даних, стають все більш вдосконаленими та складними.Забезпечення безпеки мережі стає невід'ємною частиною будь-якої організації чи користувача, які використовують цифрові технології. Способи захисту від мережевих атак охоплюють великий спектр стратегій, від технічних засобів, таких як мережеві брандмауери та системи виявлення вторгнень, до проактивних заходів, таких як аудит безпеки та навчання персоналу.Список використаних джерелhttps://holodoks.blogspot.com/2017/12/blog-post.html |