МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Захист мультимедійної мережі від DDoS-атак на основі технології DPI»

Виконавець: _____ Євгеній ЛИШТВА
(підпис)

Керівник: _____ Володимир КЛИМЧУК
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Лиштви Євгенія Юрійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Захист мультимедійної мережі від DDoS-атак на основі технології DPI»
затверджена наказом ректора від «29» березня 2023 р. № 421/ст
2. Термін виконання роботи: з 22.05.2023 р. по 25.06.2023 р.
3. Вихідні дані до роботи: аналіз сучасних DDoS-атак на мультимедійні мережі, аналіз трафіку, система моніторингу, експериментальне тестування запропонованого методу захисту, оцінка ефективності і надійності розробленого методу
4. Зміст пояснювальної записки: принцип побудови мультимедійної мережі за допомогою Cloud-технологій, розробка способу визначення початку атаки, обчислення надійності та ефективності запропонованого методу
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди презентації в програмному пакеті Microsoft PowerPoint

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	22.05.2023-24.05.2023	Виконано
2	Вступ	25.05.2023	Виконано
3	Аналіз побудови сучасних мультимедійних мереж	26.05.2023-29.05.2023	Виконано
4	Аналіз впливу DDoS-атак на сучасні мультимедійні мережі та системи	30.05.2023-07.06.2023	Виконано
5	Аналіз існуючих методів захисту мультимедійного середовища від DDoS-атак за допомогою технології DPI	08.06.2023-14.06.2023	Виконано
6	Усунення недоліків та захист кваліфікаційної роботи	15.06.2023-25.06.2023	Виконано

7. Дата видачі завдання: “19" травня 2023 р.

Керівник кваліфікаційної роботи _____ Володимир КЛИМЧУК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Євгеній ЛИШТВА
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Захист мультимедійної мережі від DDoS-атак на основі технології DPI» містить _66_ сторінок, _23_ рисунків, _15_ використаних джерел.

CLOUD-МЕРЕЖІ, DDOS-АТАКА, МЕРЕЖЕВІ СЕРВІСИ, ТРАФІК, МОНІТОРИНГ, ОБСЛУГОВУВАННЯ, МУЛЬТИМЕДІЙНІ ДАНІ, СТРІМІНГ, БІТРЕЙТ, ІДЕНТИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ, ІНФРАСТРУКТУРА, ФІЛЬТРАЦІЯ, НАВАНТАЖЕННЯ, ВТОРГНЕННЯ, АНОМАЛІЇ, АЛГОРИТМИ.

Об'єктом дослідження –. є аналіз та захист мультимедійної мережі від DDoS-атак з використанням технології DPI (Deep Packet Inspection).

Предмет дослідження –.є аналіз та розробка методів та алгоритмів захисту мультимедійних мереж від DDoS-атак з використанням технології DPI.

Мета кваліфікаційної роботи –. проаналізувати сучасні методи та технології захисту мультимедійних мереж від DDoS-атак, а також розробити ефективні методи та алгоритми захисту мультимедійної мережі на основі технології DPI.

Метод дослідження –. збір та аналіз статистичних даних: збір інформації про DDoS-атаки на мультимедійну мережу, вимірювання показників пропускної здатності, завантаженості мережі, а також аналіз типових характеристик атак та їх впливу на мережевий трафік.

Матеріали кваліфікаційної роботи рекомендується використовувати в якості підґрунтя для розробки нових методів або рішень в області захисту мультимедійних мереж від DDoS-атак. Ці матеріали можуть стати основою для подальшої розробки продуктів або систем захисту, які будуть використовуватися в індустрії.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

Deep Packet Inspection _____ (DPI)

Internet Protocol _____ (IP)

HyperText Transfer Protocol _____ (HTTP)

Domain Name System _____ (DNS)

User Datagram Protocol _____ (UDP)

Transmission Control Protocol _____ (TCP)

Software-Defined Networking_____ (SDN)

Internet Control Message Protocol _____ (ICMP)

Denial-of-Service _____ (DoS)

Distributed Denial of Service _____ (DDoS)

Quality of service _____ (QoS)

Service Set Identifier_____ (SSID)

Система виявлення вторгнень _____ (СВВ)

*Система запобігання вторгненням*_____ (СЗВ)

Intrusion Detection System _____ (IDS)

Intrusion Prevention System _____ (IPS)

Infrastructure as a Service _____ (IaaS)

Platform as a Service _____ (Paas)

Application Programming Interface _____ (API)

Voice over IP _____ (VoIP)

Internet Relay Chat _____(IRC)

Moving Picture Experts Group _____ (MPEG-2)

Joint Photographic Experts Group _____ (JPEG)

Advanced Video Coding _____ (AVC)

High Efficiency Video Coding _____ (HEVC)

ВСТУП

Актуальність теми. мультимедійні мережі є невід'ємною частиною сучасного інформаційного простору. Вони використовуються для передачі відео, аудіо, зображень та іншого мультимедійного контенту. В разі атаки на мультимедійну мережу може виникнути недоступність сервісів та серйозні фінансові збитки, втрата клієнтів, а також інші наслідки від несанкціонованого доступу до конфіденційної інформації, і в найгіршому випадку- викликати втрату даних. Це може мати негативний вплив на безпеку та конфіденційність організації та її клієнтів.

Зв’язок роботи з науковими програмами, планами, темами.

Мета і завдання дослідження. проаналізувати сучасні методи та технології захисту мультимедійних мереж від DDoS-атак, а також розробити ефективні методи та алгоритми захисту мультимедійної мережі на основі технології DPI.

Для досягнення поставленої мети вирішуються такі наукові завдання.

Об’єктом дослідження – є аналіз та захист мультимедійної мережі від DDoS-атак з використанням технології DPI (Deep Packet Inspection).

Предметом дослідження – є аналіз та розробка методів та алгоритмів захисту мультимедійних мереж від DDoS-атак з використанням технології DPI.

Методи досліджень. збір та аналіз статистичних даних: збір інформації про DDoS-атаки на мультимедійну мережу, вимірювання показників пропускної здатності, завантаженості мережі, а також аналіз типових характеристик атак та їх впливу на мережевий трафік.

Практичне значення отриманих результатів.

Об’єкти та матеріали досліджені у цій роботі - рекомендується використовувати в якості підґрунтя для розробки нових методів або рішень в області захисту мультимедійних мереж від DDoS-атак. Ці матеріали можуть стати основою для подальшої розробки продуктів або систем захисту, які будуть використовуватися в індустрії.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «ПОЛІТ. Сучасні проблеми науки», м. Київ, 2023 р.

РОЗДІЛ 1
АНАЛІЗ ПОБУДОВИ СУЧАСНИХ МУЛЬТИМЕДІЙНИХ МЕРЕЖ

1.1. Архітектура мультимедійної мережі

Архітектура мультимедійної мережі включає набір складових та протоколів, які дозволяють передавати, обробляти та отримувати різноманітні мультимедійні дані, такі як відео, аудіо та графіка, з дотриманням певних вимог до якості обслуговування. Основні компоненти такої мережі включають: Джерела мультимедіа: це джерела, які створюють або генерують мультимедійні дані, наприклад, відеокамери, мікрофони, сервери з медіа-контентом або веб-камери користувачів. Кодування та стиснення: мультимедійні дані можуть бути закодовані та стиснуті для зменшення їх обсягу та покращення ефективності передачі. Різні алгоритми стиснення, такі як MPEG, JPEG або AAC, використовуються з цією метою. Мережевий транспорт: дані передаються по мережі за допомогою протоколів передачі даних, таких як IP (Internet Protocol), TCP (Transmission Control Protocol) або UDP (User Datagram Protocol) [1]. Ці протоколи забезпечують доставку даних від одного вузла до іншого, забезпечуючи цілісність та надійність передачі. Мережеве обладнання: це включає комутатори, маршрутизатори, файрволи та інше обладнання, яке забезпечує маршрутизацію, комутацію та фільтрацію трафіку в мережі. Ці компоненти відіграють важливу роль у забезпеченні якості обслуговування та ефективності передачі мультимедійних даних.

Протоколи стрімінгу: Для передачі мультимедійних даних в режимі реального часу використовуються спеціальні протоколи стрімінгу, такі як RTP (Real-Time Transport Protocol) та RTSP (Real-Time Streaming Protocol). Їх основною метою є надійна та безперебійна доставка мультимедійних даних з мінімальними затримками.

Сервери мультимедіа: Це спеціальні сервери, які забезпечують зберігання, обробку та передачу мультимедійних даних. Вони можуть виконувати такі функції,

як кешування контенту, стрімінг в реальному часі, обробка запитів користувачів та управління мультимедійною базою даних.

Клієнтські пристрої: Це пристрої, які отримують мультимедійні дані від серверів та відтворюють їх для користувачів. Це можуть бути комп'ютери, мобільні пристрої, смарт-телевізори, плеєри та інші пристрої, що підтримують відтворення мультимедіа. Контроль пропускної здатності: Мультимедійні дані потребують певної пропускної здатності для забезпечення якісної передачі та відтворення. Механізми контролю пропускної здатності визначають, як розподілити доступну пропускну здатність мережі між різними типами трафіку, надаючи пріоритет мультимедійним даним та гарантуючи, що вони отримують достатню пропускну здатність для безперебійної передачі.

QoS (Quality of Service): Це механізми та протоколи, що забезпечують контроль якості обслуговування для мультимедійних даних [2]. Вони дозволяють приділяти пріоритети різним типам трафіку, резервувати пропускну здатність та гарантувати доставку даних з низькою затримкою та мінімальними втратами для забезпечення якісного відтворення мультимедіа. Ці механізми сприяють ефективному використанню ресурсів мережі та забезпеченню оптимального досвіду користувачів під час відтворення мультимедійних даних. В цілому, всі ці компоненти тісно взаємодіють між собою в архітектурі мультимедійної мережі, забезпечуючи передачу, обробку та відтворення мультимедійних даних з встановленими вимогами до якості обслуговування.

Безпека мультимедійної мережі є необхідною складовою її архітектури і включає різноманітні механізми та протоколи, які призначені для захисту від різних загроз безпеки. Ці загрози можуть включати атаки DDoS, перехоплення даних або несанкціонований доступ до системи. Шифрування, аутентифікація, контроль доступу та моніторинг є важливими механізмами, які допомагають забезпечити безпеку мультимедійної мережі.

Управління мультимедійною мережею є ще однією важливою складовою і включає керування ресурсами мережі, моніторинг стану мережі та вирішення проблем, які можуть виникати. Протоколи управління, такі як SNMP (Simple Network

Management Protocol), використовуються для забезпечення ефективної роботи мережі та планування ресурсів.

Механізми управління чергами є важливими для керування трафіком в мультимедійній мережі. Вони контролюють розподіл трафіку і запобігають перевантаженню мережевих вузлів. Застосовуються алгоритми планування черг для приділення пріоритетів мультимедійному трафіку та зменшення затримок.

Буферизація та адаптивність - відіграють важливу роль в мультимедійній мережі. Буферизація дозволяє компенсувати затримки та втрати пакетів шляхом тимчасового збереження мультимедійних даних на різних етапах мережі [3].

Адаптивність використовується для автоматичного змінювання параметрів передачі мультимедійних даних залежно від умов мережі та можливостей пристрою отримувача. Цей механізм дозволяє оптимізувати якість відтворення, забезпечуючи максимально можливу якість при наявності достатніх ресурсів, а також знижуючи якість у разі обмежених ресурсів для запобігання затримкам або відтворенню з перебоями.

Одним із параметрів, який може бути адаптований, є роздільна здатність. В залежності від пропускної здатності мережі та можливостей пристрою отримувача, роздільна здатність може бути знижена або підвищена. Наприклад, при обмежених ресурсах мережі або пристрою з низькою швидкістю Інтернету може бути використана менша роздільна здатність для зниження обсягу передаваних даних і покращення відтворення.

Бітрейт є ще одним параметром, який може бути адаптований. В залежності від доступної пропускної здатності мережі може бути змінений бітрейт передачі мультимедійних даних. При великій пропускній здатності може бути використаний високий бітрейт для забезпечення високоякісного відтворення, тоді як при обмежених ресурсах може бути знижений бітрейт для зменшення обсягу даних і забезпечення безперебійного відтворення.

Крім того, адаптивність також стосується вибору кодеку або аудіо-відео формату. Різні кодеки мультимедійних даних мають різні вимоги до обчислювальних ресурсів та пропускної здатності мережі. Кодеки використовуються для стиснення та

розкодування аудіо-відео даних з метою зменшення їх обсягу для передачі та збереження.

Деякі кодеки, наприклад, H.264 або H.265 (також відомий як AVC або HEVC), забезпечують високу ступінь стиснення та якість відтворення, але вимагають більше обчислювальних ресурсів для кодування та декодування [4]. Такі кодеки можуть бути використані, наприклад, при потоковій передачі відео високої якості на пристрої з великою обчислювальною потужністю та швидким Інтернет-з'єднанням.

У той же час, існують кодеки, які забезпечують меншу ступінь стиснення та вимагають менше обчислювальних ресурсів для кодування та декодування, наприклад, MPEG-2 або JPEG. Ці кодеки можуть бути використані, наприклад, у випадках, коли пропускна здатність мережі обмежена або пристрій отримувача має обмежені обчислювальні можливості. Адаптивність полягає у виборі оптимального кодеку залежно від умов мережі та можливостей пристрою отримувача. В деяких випадках може бути використана автоматична зміна кодеку під час передачі мультимедійних даних з метою досягнення оптимальної якості відтворення при мінімальних вимогах до ресурсів.

В цілому, адаптивність кодеків, разом з адаптивністю роздільної здатності та бітрейту, допомагає забезпечити оптимальне відтворення мультимедійних даних в реальному часі з урахуванням умов мережі та можливостей пристрою отримувача. Це дозволяє досягти балансу між якістю відтворення, ефективністю передачі даних та задоволенням користувачів.

Під час передачі мультимедійних даних, система може періодично аналізувати умови мережі, такі як пропускна здатність та затримки, а також можливості пристрою отримувача. На основі цієї інформації може бути прийняте рішення щодо вибору оптимального кодеку, роздільної здатності та бітрейту для передачі. Наприклад, якщо умови мережі стають обмеженими, система може знизити роздільну здатність або бітрейт для забезпечення плавного відтворення при низькій пропускній здатності. За необхідності, кодек може бути замінений на менш обчислювально-інтенсивний варіант, що дозволить зменшити навантаження на пристрій отримувача.

У разі поліпшення умов мережі, система може автоматично підвищити роздільну здатність або бітрейт для досягнення вищої якості відтворення. Кодек може бути замінений на більш потужний, який забезпечить більш ефективне стиснення та якість зображення. Застосування адаптивності параметрів передачі, таких як кодек, роздільна здатність та бітрейт, дозволяє мультимедійним мережам підлаштовуватись до змінних умов мережі та ресурсів пристроїв, забезпечуючи оптимальне відтворення мультимедійних даних та задоволення користувачів.

Моніторинг та керування: для оптимального функціонування мультимедійної мережі важливо мати механізми, які дозволяють виявляти та вирішувати різні проблеми, такі як перевантаження, втрати пакетів або знижена якість обслуговування. Моніторинг надає можливість збирати дані про стан мережі, пропускну здатність, затримки та інші параметри для подальшого аналізу та оптимізації роботи мультимедійної мережі. Керування, з свого боку, включає можливості для зміни налаштувань мережі, резервування ресурсів та прийняття оптимальних рішень з метою забезпечення високої якості обслуговування.

Скалінг та резервування ресурсів: мультимедійні мережі повинні бути гнучкими та масштабованими, щоб впоратися з ростом обсягу трафіку та забезпечити надійну якість обслуговування. Механізми скалінгу дозволяють додавати або зменшувати ресурси мережі в залежності від потреб трафіку. Резервування ресурсів дозволяє виділяти достатню пропускну здатність, обчислювальні ресурси та пам'ять для забезпечення надійної якості обслуговування мультимедійних даних.

Ідентифікація та аутентифікація: мультимедійна мережа може використовувати механізми ідентифікації та аутентифікації для забезпечення безпеки та контролю доступу до мультимедійних ресурсів. Це можуть бути механізми аутентифікації користувачів, шифрування даних та захисту від несанкціонованого доступу.

Рис.1.1 Класифікація комп’ютерних мереж

Ці компоненти та протоколи взаємодіють, щоб створити ефективну та надійну мультимедійну мережу, яка забезпечує передачу, обробку та відтворення мультимедійних даних з високою якістю обслуговування та забезпечує безпеку. Залежно від конкретних вимог та сценаріїв використання мультимедійної мережі, архітектура може варіюватися [5].

1.2 Хмарні обчислювальні середовища

Хмарні обчислення - одна з передових технологій, яка дозволяє отримати величезний обсяг зберігання даних та надання послуг, в той же час вони пропонують високу продуктивність і низьку вартість. Хмарні обчислення, відомі як обчислювальна модель, яка керує діапазоном обчислювальних ресурсів з можливістю гнучкого налаштування. На основі моделей розгортання хмарні обчислювальні середовища можна класифікувати як середовища з публічним доступом, середовища з обмеженим доступом та гібридні середовища. Хмарні обчислювальні середовища стали легкими мішенями для зловмисників для заволодіння інформацією користувачів. DoS-атаки є найбільшою загрозою для цієї галузі обчислень і

найбільшою перешкодою для широкого впровадження хмарних обчислювальних середовищ. DOS-атаки вважаються одними з найбільш значущих проблем, що стоять перед зростанням популярності хмарних середовищ. Кілька причин роблять DoS-атаки серйозною загрозою: наприклад, така атака є руйнівною в цьому середовищі, і її легко здійснити. Крім того, зловмисники використовують підроблені IP-адреси, таким чином, відстежувати джерело нападу стає важко.

1.2.1 *Хмарні технології*

Хмарні обчислення та технології набирають популярності не тільки в комерційних проєктах, а й в освітньому процесі.

Термін "хмарні обчислення" (англ. - Cloud Computing) може бути застосований для будь-яких сервісів, які надаються через мережу Інтернет. Суть хмарних технологій полягає в наданні користувачам віддаленого доступу до послуг, обчислювальних ресурсів і додатків (включно з операційними системами та інфраструктурою) через Інтернет.

Розвиток цієї сфери хостингу (Хостинг-послуга з розміщення устаткування клієнта на території провайдера із забезпеченням підключення його до каналів зв'язку з високою пропускною спроможністю) був зумовлений потребою, що виникла, у програмному забезпеченні та цифрових послугах, якими можна було б керувати зсередини, але які були б при цьому більш економічними та ефективними. Сервіси, що входять до хмарних технологій, надаються на основі передплати або плати за використання послуги, в режимі реального часу через Інтернет, що розширює наявні можливості кінцевого користувача.

Концепції проєктів, які можна вважати прабатьками "хмарних" сервісів, з'явилися в 70-х роках минулого століття, розробники програмного забезпечення запропонували таку модель застосунків, за яких усі обчислення та обробка інформації здійснюються не на комп'ютері користувача, а на віддалених серверах. Глобальної мережі Інтернет на той час не існувало, тому перші ідеї "хмар" виявилися важко реалізовуваними і практично не використовувалися при створенні нових програм. Всерйоз технологією зацікавилися 2006 року, коли компанія Amazon представила

своїм клієнтам розгалужену систему веб-сервісів. Принципова відмінність нової інфраструктури полягала в тому, що користувачі отримували в розпорядження не тільки хостинг для зберігання даних, а й обчислювальні потужності серверів, що належать Amazon. Через рік схожі послуги запропонували флагмани IT-індустрії: Google, Sun і IBM. А ще через рік Microsoft анонсувала не просто застосунок цілу операційну систему, створену на базі "хмарної" моделі обчислень.

Існує 4 типи хмар:

Приватна хмара - інфраструктура, призначена для використання однією організацією, що включає кілька споживачів (наприклад, підрозділів однієї організації). Приватна хмара може перебувати у власності, управлінні та експлуатації як самої організації, так і третьої сторони (або будь-якої їхньої комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника;

Публічна хмара (англ. public cloud) - інфраструктура, призначена для вільного використання широкою публікою. Публічна хмара може перебувати у власності, управлінні та експлуатації комерційних, наукових та урядових організацій (або будь-якої їх комбінації). Публічна хмара фізично існує в юрисдикції власника - постачальника послуг;

Гібридна хмара (англ. hybrid cloud) - це комбінація з двох або більше різних хмарних інфраструктур (приватних, публічних), що залишаються унікальними об'єктами, але пов'язані між собою стандартизованими або приватними технологіями передавання даних і застосунків (наприклад, короткочасне використання ресурсів публічних хмар для балансування навантаження між хмарами);

Громадська хмара (англ. community cloud) - вид інфраструктури, призначений для використання конкретною спільнотою споживачів з організацій, що мають спільні завдання. Громадська хмара може перебувати в кооперативній (спільній) власності, управлінні та експлуатації однієї або більше з організацій спільноти або третьої сторони (або будь-якої їхньої комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника;

На практиці межі між усіма цими типами обчислень розмиті. На малюнку 1.2 зображено 3 рівні хмарних технологій:

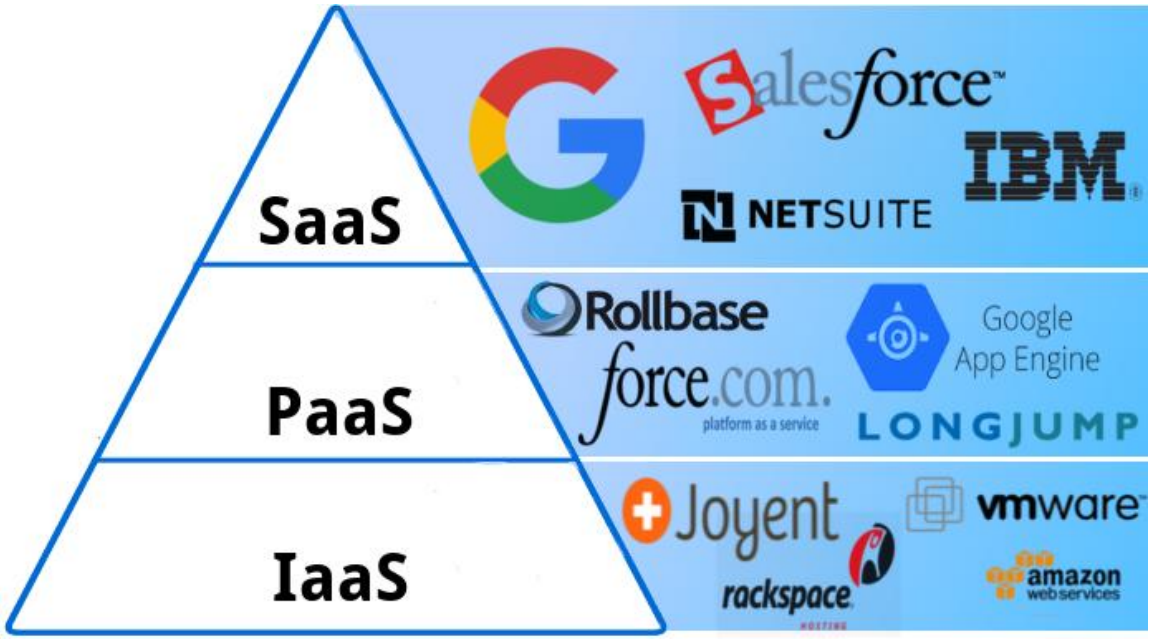


Рис. 1.2 Рівні хмарних технологій

1) інфраструктура як сервіс (Infrastructure as a Service). Інфраструктура в оренду. IaaS - це надання за запитом необхідної споживачеві кількості динамічних ресурсів (обчислювальних і сховища), віртуальних серверів, мережевої інфраструктури, віддалених робочих місць на основі концепції хмарних обчислень. Iaas дає змогу максимально оптимізувати використання орендованих потужностей. Користувачеві надається "чистий" екземпляр віртуального сервера з унікальною IP-адресою або набором адрес і частина системи зберігання даних. Для управління параметрами, запуском, зупинкою цього екземпляра провайдер надає користувачеві програмний інтерфейс (API);

2) платформа як сервіс (Platform as a Service). Paas - "платформа як послуга", модель надання хмарних обчислень [6]. Споживач цієї платформи отримує доступ до використання інформаційно-технологічних платформ. Уся інфраструктура цієї моделі цілком управляється провайдером, провайдер визначає доступ, а споживач експлуатує доступні функції, водночас динамічно змінюючи кількість споживаних обчислювальних ресурсів. PaaS можна уявити, як готову до роботи віртуальну платформу, що складається з одного або декількох віртуальних серверів зі встановленими операційними системами та спеціалізованими додатками. Більшість хмарних провайдерів пропонують користувачеві вибір з маси готових до

використання хмарних середовищ. До числа найбільших провайдерів світового ринку публічних PaaS входять IBM, VMWare, Microsoft і Google;

3) програмне забезпечення як сервіс (Software as a Service). Програмне забезпечення як послуга. SaaS - бізнес-модель, за якої розробник або постачальник веб-додатка керує ним, надаючи замовникам доступ до програмного забезпечення через Інтернет. SaaS провайдер піклується про працездатність додатка, здійснює технічну підтримку користувачів, самостійно встановлює оновлення. Концепція SaaS надає можливість користуватися програмним забезпеченням як послугою і робити це віддалено через Інтернет. Цей підхід дає змогу не купувати програмний продукт, а просто тимчасово скористатися ним у разі виникнення потреби.

Бізнес-модель SaaS має кілька переваг над традиційним програмним забезпеченням:

- нижча вартість володіння;
- коротші терміни впровадження;
- низький поріг входу (можна швидко і безкоштовно протестувати);
- завдання з підтримки та оновлення системи повністю лягають на плечі SaaS-провайдера;
- повна мобільність користувача, обмежена лише "інтернет-покриттям";
- підтримка географічно розподілених компаній і віддалених співробітників;
- низькі вимоги до потужності комп'ютера користувача.

Недоліками SaaS вважаються небезпека передачі комерційних даних сторонньому провайдеру, невисока швидкодія і ненадійність доступу через перебої з інтернетом. Однак імідж SaaS провайдерів, що зміцнюється, розвиток технологій шифрування і широкосмугового доступу до інтернету поступово розсіюють ці страхи.

Хмарні обчислення, мають свої переваги:

- користувач оплачує послугу тільки тоді, коли вона йому необхідна, а найголовніше він платить тільки за те, що використовує;

- хмарні технології дають змогу економити на придбанні, підтримці, модернізації ПЗ та обладнання;
- масштабованість, відмовостійкість і безпека - автоматичне виділення і звільнення необхідних ресурсів залежно від потреб програми. Технічне обслуговування, оновлення ПЗ здійснює провайдер послуг;
- віддалений доступ до даних у хмарі - працювати можна з будь-якої точки на планеті, де є доступ до мережі Інтернет.

Але також існують і недоліки:

- користувач не є власником і не має доступу до внутрішньої хмарної інфраструктури. Збереження користувацьких даних сильно залежить від компанії провайдера;
- недолік, актуальний для користувачів: для отримання якісних послуг користувачеві необхідно мати надійний і швидкий доступ до мережі Інтернет;
- не всі дані можна довірити провайдеру в Інтернеті не тільки для зберігання, а й навіть для обробки;
- не кожен додаток дає змогу зберегти, наприклад, на флешку проміжні етапи опрацювання інформації, а також кінцевий результат роботи, але ж онлайнові результати зручні не завжди;
- є ризик, що провайдер онлайнових сервісів одного разу не зробить резервну копію даних, і вони будуть загублені внаслідок краху сервера;
- довіряючи свої дані онлайн-сервісу, ви втрачаєте над ними контроль і обмежуєте свою свободу (користувач не матиме змоги змінити якусь частину своєї інформації, вона зберігатиметься в умовах, не підвладних йому).

Отже, хмарні ресурси мають низку переваг щодо своєї гнучкості, а також деякі недоліки в доступності.

ВИСНОВКИ ДО РОЗДІЛУ 1

В ході аналізу та дослідження хмарних технологій було виявлено, що вони є актуальним та перспективним напрямком розвитку інформаційних систем. Хмарні технології надають можливість ефективного розподілу ресурсів, забезпечують гнучкість та масштабованість, спрощують управління та забезпечують широкий доступ до обчислювальних, зберігальних та мережевих послуг.

Основними перевагами використання хмарних технологій є зниження витрат на придбання та підтримку інфраструктури, прискорення розгортання та впровадження нових сервісів, забезпечення високої доступності та надійності системи, а також забезпечення глобального доступу до даних та можливості спільної роботи з ними.

Однак, під час дослідження було виявлено й деякі виклики та проблеми, пов'язані з хмарними технологіями. Зокрема, це питання безпеки та конфіденційності даних, нестабільність мережі, проблеми інтеграції з існуючими системами та стандартами, а також віддалене керування та нагляд за інфраструктурою.

Автоматизація процесів управління хмарними сервісами має велике значення для забезпечення ефективності та оптимального використання ресурсів. Впровадження автоматичного масштабування, балансування навантаження, моніторингу та керування ресурсами дозволить підтримувати високу продуктивність системи та задовольняти зростаючі потреби користувачів.

Подальший розвиток управління хмарними сервісами також повинен враховувати аспекти безпеки. Забезпечення конфіденційності, цілісності та доступності даних є важливими аспектами при використанні хмарних технологій. Розробка ефективних механізмів шифрування, автентифікації, контролю доступу та моніторингу допоможе забезпечити захист інформації в хмарних середовищах.

Загалом, хмарні технології є перспективним інструментом для оптимізації ресурсів та забезпечення широкого доступу до послуг. Продовження досліджень і розробка нових підходів до стандартизації, автоматизації та безпеки хмарних

сервісів відкривають багато можливостей для вдосконалення хмарних інфраструктур і забезпечення їхньої широкої придатності для використання у різних сферах діяльності. Враховуючи потенціал та переваги хмарних технологій, важливо удосконалювати існуючі методи та розробляти нові підходи до забезпечення безпеки, надійності та ефективності хмарних інфраструктур. Також потрібно продовжувати дослідження в галузі стандартизації, автоматизації та управління хмарними сервісами для забезпечення їхньої ефективності та використання в різних сферах діяльності. Необхідно розробляти стандарти, які сприятимуть сумісності та інтеграції різних хмарних платформ, що дозволить користувачам вільно переміщати свої дані та сервіси між різними провайдерами.

РОЗДІЛ 2
АНАЛІЗ ВПЛИВУ DDoS-АТАК НА СУЧАСНІ МУЛЬТИМЕДІЙНІ МЕРЕЖІ ТА СИСТЕМИ

2.1 Вплив Dos-атак на мережі передачі інформації та Cloud-середовища

Правопорушники мають змогу здійснювати різноманітні DoS-атаки, які можуть спрямовуватись на приватні, загальнодоступні або будь-які типи мереж. Певні типи таких атак, мають на меті завдати шкоди ресурсам, таким як пропускна здатність мережі, пам'ять і процесор, а також націлитися на додатки, такі як служби баз даних і веб-додатки. DoS-атаки здійснюються шляхом генерації великого обсягу небажаного мережевого трафіку або застосування методів, що змушують обчислювальні ресурси обробляти фейкові процеси та зберігати дані. Ці атаки можуть мати три види впливу:

- Пряме блокування обслуговування (Direct Denial of Service): той вид, коли операційна система хмарного обчислювального середовища розглядає додаткове навантаження на певну службу як спробу зловмисника зробити її несправною [7].

- Непряме блокування обслуговування (Indirect Denial of Service): вид атаки, яка спрямована на обчислювальну потужність [8]. Відносно негативний вплив прямої атаки досягається шляхом перевантаження нерелевантною інформацією однієї служби, що має вплив на інші служби, які працюють на тих самих обчислювальних ресурсах. Ці інші служби можуть страждати від навантаження, спричиненого атакою на іншу службу. Таким чином, якщо, наприклад, декілька служб працюють на одному обчислювальному ресурсі, то атака на одну з них може вплинути на загальну доступність всіх інших служб.

Головним наслідком атаки з перенасиченням нерелевантною інформацією (flooding) на хмарних потужностях є стягнення плати з клієнтів за використання ресурсів, не обмежуючи при цьому обчислювальну потужність.

Основні хмарні обчислення мають певні характеристики, що впливають на захист від атак типу DoS. Найяскравіші методи захисту можна узагальнити в трьох поняттях: ідентифікація, виявлення і фільтрація. В першому випадку, фізичні сервери в хмарних обчислювальних середовищах управляють мережевими і обчислювальними ресурсами замість користувачів, що робить їх менш вразливими до атак. В другому випадку, виділення ресурсів і міграція віртуальних машин представляють нові джерела змін у мережевій топології, і процеси цих змін швидко розвиваються. Тому захист від атак типу DoS має бути налаштований для динамічної мережі з частими змінами топології, здатний виявляти швидко і реагувати негайно. В наступному випадку, хмарні обчислення дозволяють всім користувачам спільно використовувати мережеву інфраструктуру, тому необхідно надійно розділяти мережу. Традиційні методи захисту від атак типу DoS не враховують ці вимоги. Операції виявлення і захисту від атак типу DoS не повинні впливати на роботу мережі і користувачів, а також користувачі не повинні впливати на ці операції.

Опційна модель хмарних середовищ викликала нові виклики для атак типу DDoS, такі як динамічна мережева топологія та розширений периметр оборони. Для успішного розв'язання цих проблем адміністратор хмарного середовища повинен мати можливість просто делегувати управління мережею користувачам хмари і швидко налаштовувати керування на основі змін у топології мережі. SDN (Software-Defined Networking) забезпечує розширену логіку виявлення та легко впроваджує ефективні операції, а також забезпечує швидку обробку пакетів. У той же час, затримки в мережі та потоці трафіку, що виникають у зв'язку з керуванням мережею та змінами в топології, наприклад, взаємодія між захисними схемами від DDoS та комутаторами, можуть створювати нові хвилі атак та призводити до відмови в певних точках мережі. Щоб уникнути нових вразливостей у сфері безпеки, необхідно враховувати втрати обчислювальних ресурсів та комунікаційні витрати при розробці рішень для захисту від атак типу DDoS. Загалом, мультимедійні мережі можуть мати перевагу в захисті хмарних середовищ та мереж передачі даних від атак типу DDoS, коли всі комунікаційні та обчислювальні процеси належним чином налаштовані та оптимізовані.

2.2 Структура та основні принципи DDoS-атак

DDoS-атака, яка є розподіленою атакою на відмову в обслуговуванні, є шкідливою дією, метою якої є порушення нормального функціонування цільового сервера, послуги або мережі шляхом перенасичення їх потоком Інтернет-трафіку [9]. Щоб досягти своєї мети, DDoS-атаки використовують кілька скомпрометованих комп'ютерних систем як джерело атакуючого трафіку. Ці компрометовані машини можуть включати в себе як комп'ютери, так і різноманітні мережеві ресурси, включаючи пристрої Інтернету речей (IoT).

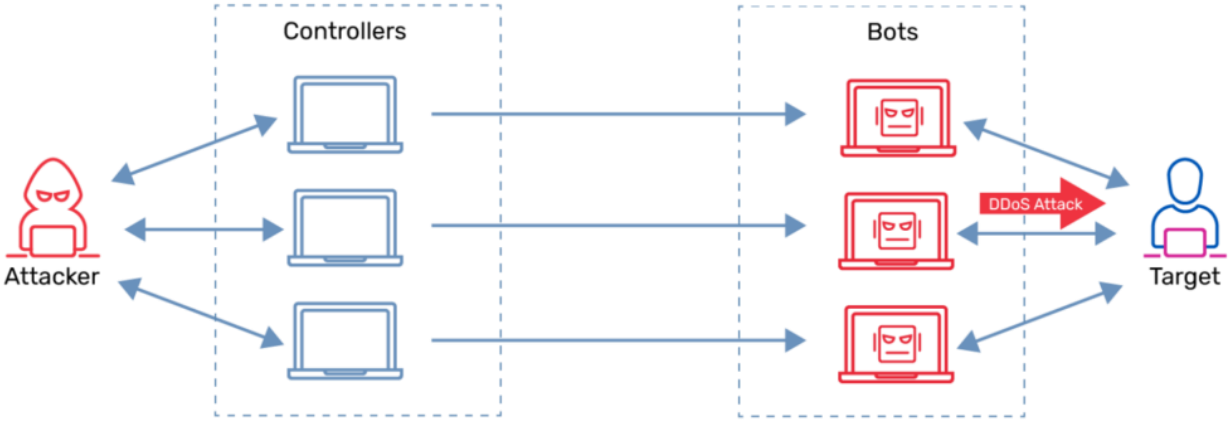


Рис. 2.1 Узагальнений вигляд використання вражених пристроїв

Дані мережі складаються з комп'ютерів та інших пристроїв, таких як пристрої Інтернету речей (IoT), які були заражені шкідливим програмним забезпеченням і можуть бути дистанційно керовані зловмисником. Окремі пристрої називають ботами, а колективну групу таких ботів називають бот-мережею. Після створення бот-мережі зловмисник може надсилати віддалені команди кожному боту для здійснення атаки.

Коли бот-мережа спрямовується на сервер або мережу жертви, кожен бот надсилає запити до IP-адреси цілі, що може призвести до надмірного завантаження сервера або мережі і, в результаті, до відмови в обслуговуванні звичайного трафіку. Оскільки кожен бот є законним пристроєм Інтернету, розрізнення атакуючого трафіку від нормального може бути важкою задачею.

Найочевиднішим натяком на DDoS-атаку є раптове сповільнення або недоступність сайту або сервісу. Проте, оскільки існує кілька причин, таких як легітимний зріст трафіку, які можуть спричинити подібні проблеми з продуктивністю, зазвичай необхідне подальше розслідування. Певні інструменти аналізу трафіку можуть допомогти виявити деякі характерні ознаки DDoS-атаки:

- Надмірний обсяг трафіку, що надходить з однієї IP-адреси або діапазону IP.
- Неочікуваний ріст запитів до конкретної сторінки або кінцевої точки.
- Підозрілі або незвичайні запити, що містять специфічні ключові слова, параметри або шаблони.
- Потік трафіку від користувачів з аналогічними поведінковими характеристиками, такими як тип пристрою, геолокація або версія веб-браузера.
- Неординарні шаблони руху, такі як активність в непритаманний час або схеми, що видаються неестетичними (наприклад, регулярні скачки кожні 10 хвилин).
- Велика кількість запитів з однієї або кількох IP-адрес, які не відповідають звичайним користувачам або необхідним ботам (наприклад, пошукові роботи).

Ці ознаки можуть свідчити про наявність DDoS-атаки і допомогти виявити зловмисника. Важливо мати в своєму розпорядженні інструменти трафік-аналізу, які дозволяють виявити та реагувати на подібні атаки, забезпечуючи надійний захист і нормальне функціонування мережі чи сервера.

Хоча майже всі DDoS-атаки спрямовані на переповнення цільового пристрою або мережі трафіком, їх можна поділити на три категорії. Зловмисники використовують один або декілька різних векторів атаки або циклюють вектори атаки відповідно до контрзаходів.

Перша категорія - атаки на основі об'єму. При цьому використовуються потоки UDP (User Datagram Protocol), які атакують випадкові порти на віддаленому сервері за допомогою UDP-пакетів. Система перевіряє порти на відповідні

програми, і якщо жодної програми не знаходиться, сервер відправляє пакет "недоступний для призначення". Отриманий трафік може переповнити послугу.

Друга категорія - поток ICMP (ping). При цьому використовуються пакети ехо-запиту (ping) протоколу керування Інтернетом (ICMP) до хосту. Пінги використовуються для вимірювання з'єднання між двома серверами. Зловмисник відправляє велику серію пінгів, щоб вичерпати пропускну здатність цільового сервера.

Третя категорія - об'ємні DDoS-атаки, коли зловмисники засипають жертву великим обсягом пакетів або з'єднань, часто використовуючи мережеве обладнання, сервери або ресурси пропускної здатності. Це найбільш поширені типи DDoS-атак. Раніше об'ємні атаки здійснювалися за допомогою багатьох скомпрометованих систем, що належали бот-мережам. Зараз хакери не лише використовують традиційні методи атак, але також залучають добровольців для здійснення атак з їх власних машин. Крім того, нові центри величезних об'ємних атак зараз запускаються з центрів обробки даних провайдерів хмарних послуг. Зловмисники орендують або компрометують хмарні системи, які мають величезну пропускну здатність Інтернету. Це надає їм можливість здійснювати масштабні атаки з великою потужністю і значною швидкістю передачі даних. Використання цих хмарних центрів дозволяє зловмисникам маскувати свою діяльність і ускладнює виявлення та блокування атак.

Такі об'ємні DDoS-атаки можуть значно вплинути на функціонування цільових систем, призводячи до перевантаження мережі, недоступності ресурсів та значних витрат на відновлення послуг. Розробники захисних рішень та провайдери мережевої безпеки постійно працюють над вдосконаленням методів виявлення і захисту від таких атак, включаючи аналіз трафіку, виявлення аномальних активностей та використання спеціалізованих апаратних і програмних засобів.

Поняття ботнет - це сукупність підключених до Інтернету скомпрометованих систем, яка може використовуватися для різноманітних незаконних дій, таких як надсилання спаму електронною поштою, участь в DDoS-атаках або виконання інших злочинних завдань [11]. Термін "ботнет" походить від поєднання слів "робот" і

"мережа". Системи, що підпадають під контроль зловмисників, часто називаються "зомбі". Зомбі можуть бути скомпрометовані через обман користувачів, шляхом використання вразливостей веб-браузерів або шляхом переконання користувача запустити шкідливу програму, наприклад, троянський коней. На рисунку 2.2 зображено типову структуру ботнету.

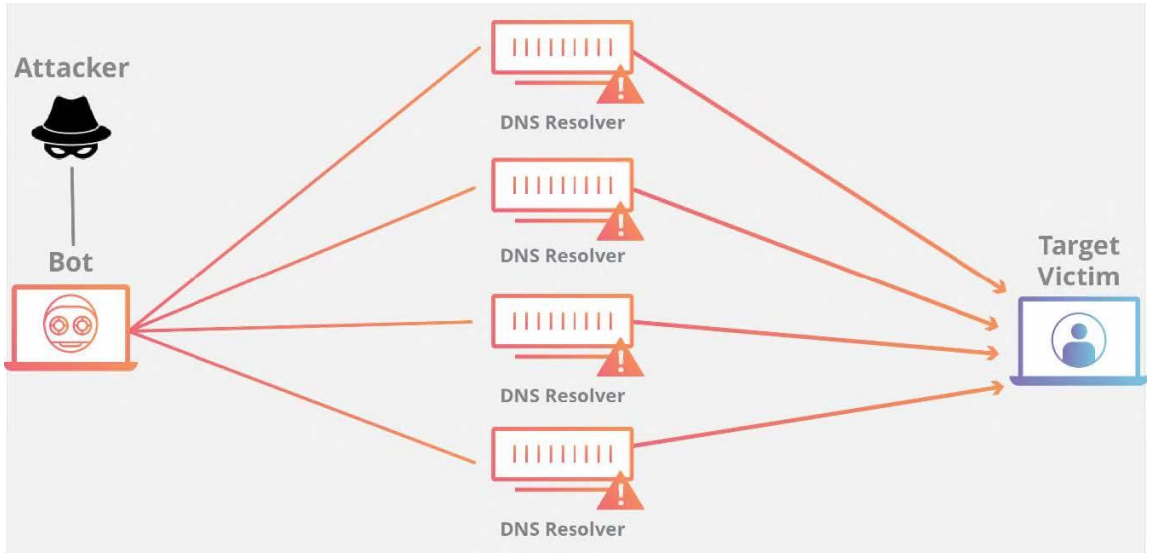


Рис. 2.2 Атаки на основі ботнету

У даному прикладі, зловмисник використовує зомбі для здійснення DDoS-атаки на інфраструктуру жертви. Ці зомбі встановлюють прихований канал зв'язку з сервером управління, яким зловмисник керує. Часто ця комунікація здійснюється за допомогою Інтернет-ретрансляційних чатів (IRC), зашифрованих каналів, спеціальних однорангових мереж або навіть через Twitter.

З появою хмарних послуг та провайдерів на ринку стали спостерігатися нові тенденції. Зловмисники активно орендують або незаконно отримують доступ до потужних обчислювальних ресурсів та хмарних серверів з метою здійснення DDoS-атак. Хмарні обчислення, які розширюють можливості для законних організацій, також стають привабливою платформою для кіберзлочинців, оскільки це вигідно та зручно дозволяє їм використовувати потужні обчислювальні ресурси для вчинення злочинних дій. Ця концепція показана на рис. 3.3.

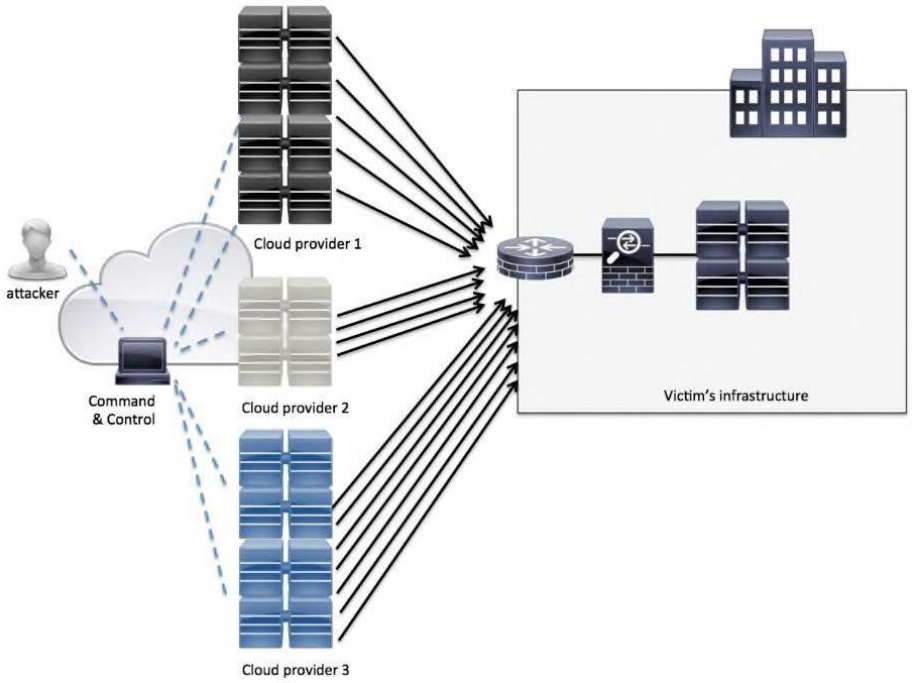


Рис. 2.3 Компрометовані хмарні сервери

Атаки на інфраструктуру DNS, які спрямовані на зміцнення серверів, мають свої особливості. Під час взаємодії з системою доменних імен (DNS), запити можуть бути рекурсивними або нерекурсивними (ітеративними). Зазвичай клієнтські програми, такі як веб-браузери, вимагають виконання рекурсії з боку DNS-сервера, встановлюючи прапорець рекурсії (RD) у пакеті DNS-запиту. Якщо DNS-сервер не може задовольнити запит з кешу або з власної зони, він буде звертатися до інших DNS-серверів. На жаль, багато рекурсивних DNS-серверів допускають запити DNS з будь-якого джерела. Крім того, багато реалізацій DNS за замовчуванням дозволяють виконання рекурсії, навіть якщо сервер імен призначений лише для авторитетних запитів. Цей тип сервера відомий як "відкритий резольвер". Відкриті резольвери DNS є вразливими до різних шкідливих атак, таких як отруєння кешу DNS та DDoS-атаки.

Атака на посилення DNS є найпоширенішою формою DDoS-атак і використовує рекурсивні DNS-сервери, хоча деякі атаки на посилення DNS можуть бути успішними навіть без використання рекурсивних серверів. Атаки на посилення DNS подібні до атак smurf. У випадку атаки smurf зловмисник надсилає фальшиві ICMP-запити exo (тип 8) для створення умов DoS. У випадку атаки на посилення

DNS зловмисник надсилає невеликі фальшиві запити адреси до відкритого резольвера, змушуючи його надсилати значно більші відповіді на підроблену адресу. Після цього резольвер стає сприячим DDoS-атаки на підроблені адреси. Атаки на посилення DNS наведені на рисунку 2.4 ілюструють основні етапи DDoS-атаки. Зловмисник, використовуючи цю стратегію, надсилає фальшиві запити до відкритого резольвера. Ці запити, хоча й невеликі, містять підроблену адресу, що спонукає резольвер надсилати значно більші відповіді на цю адресу. В результаті резольвер стає активним учасником DDoS-атаки, сприяючи заливтю підробленої адреси великими обсягами трафіку. Така атака може викликати серйозне перевантаження і відмову в обслуговуванні цільового сервера або мережі.

Поява атак на посилення DNS є особливо небезпечною, оскільки вони використовують вразливості рекурсивних серверів імен та можуть призвести до значного збільшення обсягу трафіку, що направляється на цільовий об'єкт [12]. Це може спричинити серйозні проблеми з доступністю та функціонуванням інтернет-ресурсів.

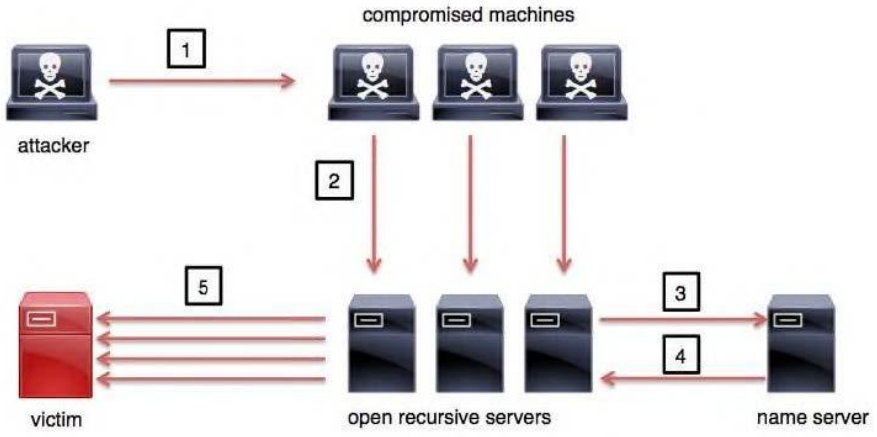


Рис. 2.4 - Атака посилення DNS

Наступні етапи, які проілюстровані на рисунку 2.4, включають:

1. Правопорушник ініціює та керує скомпрометованими машинами для запуску атаки.

2. Компрометовані машини відправляють DNS-запит до домену example.com і змінюють вихідну IP-адресу на IP-адресу жертви.

3. Відкриті резольвери запитують верхні DNS-сервери щодо розташування example.com.

4. Сервер імен надсилає відповідь назад до відкритих рекурсивних серверів.

5. Відкриті рекурсивні сервери надсилають DNS-відповіді до жертви.

Атаки на рівні додатків, такі як атаки HTTP-потоку, є атаками на рівні 7 додатків, які використовують бот-мережі, часто відомі як "армія зомбі". Під час цих атак, стандартні запити GET та POST надсилаються до веб-сервера або додатку з метою перевантаження. Це може призводити до перевантаження сервера та його відмови в обслуговуванні. Оскільки ці атаки схожі на нормальний трафік, їх виявлення може бути складним.

З другої сторони, інші програми, такі як Voice over IP (VoIP), DNS та інші, часто також стають об'єктом атак.

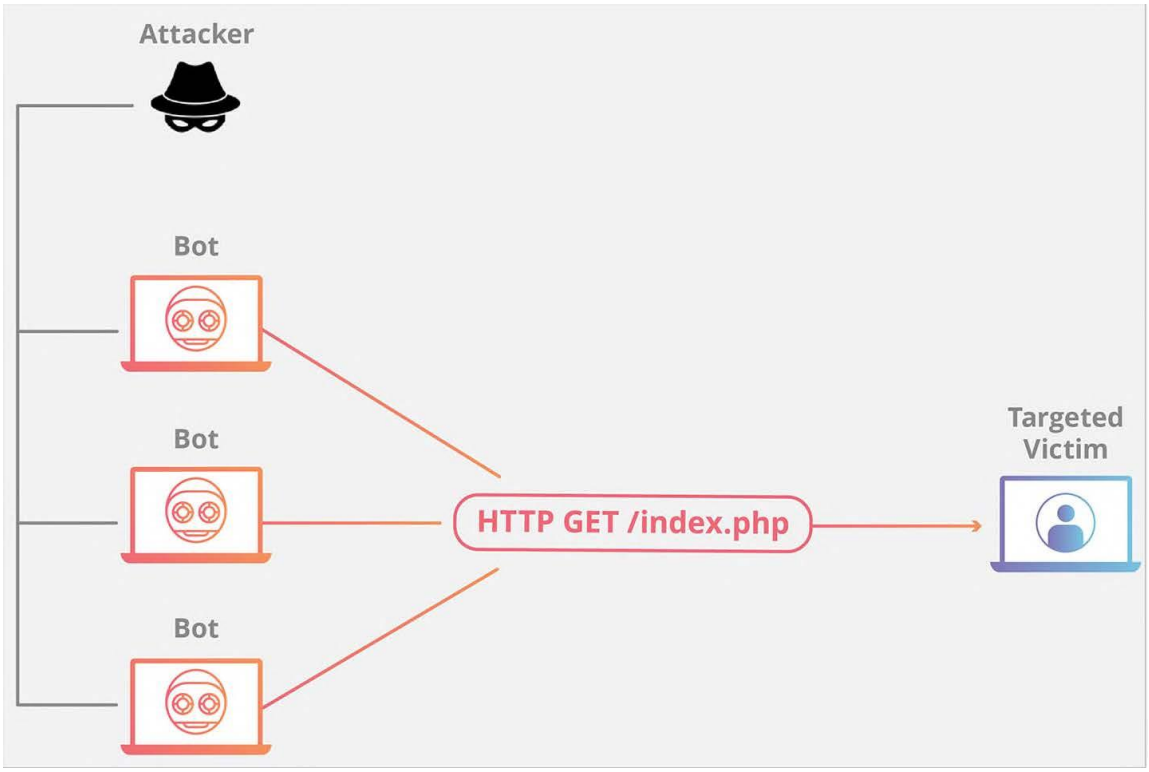


Рис. 2.5 - Атаки на рівні додатків

DDoS-атаки, спрямовані на програми, можуть бути націлені на різноманітні додатки. Однак найпоширенішою цільовою точкою є HTTP, яке призначене для вичерпання веб-серверів та служб. Деякі з таких атак виявляються більш ефективними за інші, оскільки для досягнення своєї мети вони вимагають меншої кількості мережевих з’єднань. Наприклад, зловмисник може запустити безліч запитів HTTP GET або POST, щоб перевантажити веб-сервер або веб-програму [13].

Пояснення можливості здійснення повільних DoS-атак пов'язано з особливостями протоколу TCP в Інтернеті, зокрема з його механізмом тайм-ауту та повторної передачі пакетів. Цей механізм працює наступним чином: після відправлення пакету очікується певний час (RTO - Retransmission TimeOut) на отримання пакету-відповіді. Зловмисники використовують цю особливість для здійснення атак. Вони надсилають трафік у формі імпульсів в кінці кожного інтервалу RTO. Це призводить до перевантаження каналу зв'язку під час очікування пакету-відповіді, що призводить до його недоставки. Після цього процес повторюється знову. Таким чином, система стає недоступною. Графічне зображення повільної DoS-атаки, отримане під час експериментального дослідження, можна побачити на рисунку 2.6.

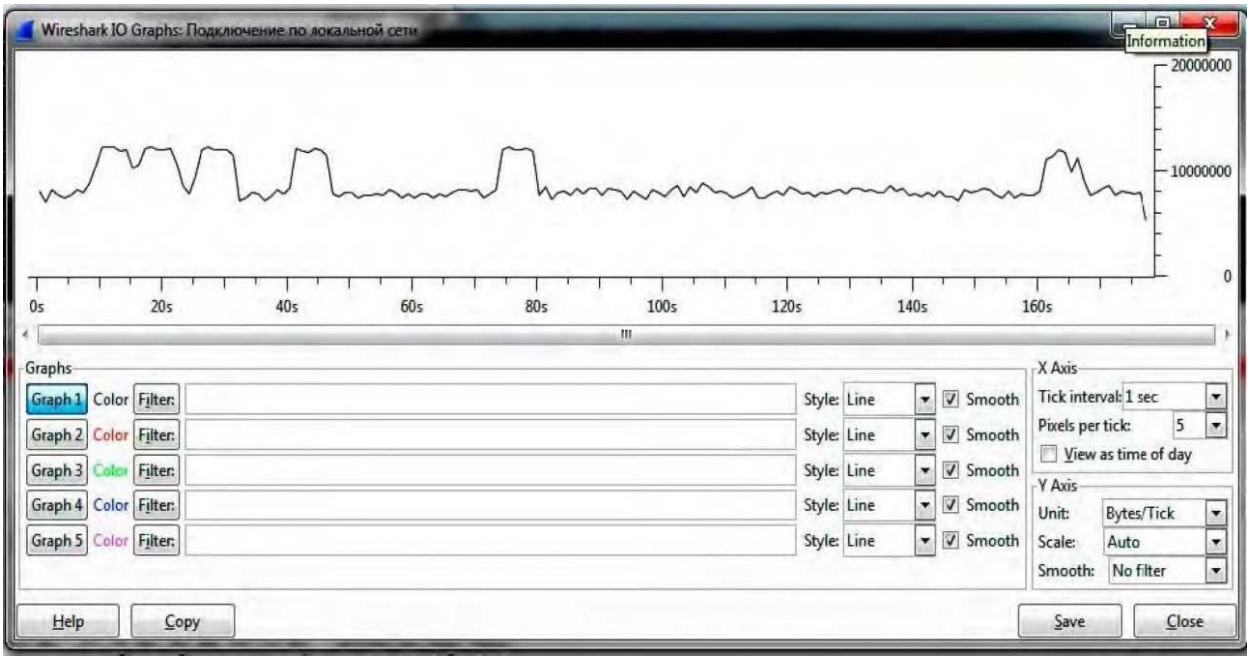


Рис. 2.6 - Графічне зображення повільної DoS-атаки

Фундаментальним методом для виявлення повільних DoS-атак є відстеження контрольних характеристик трафіку в умовах максимального завантаження мережі та подальший аналіз аномалій у його структурі. Аномалія - це відхилення від звичайної структури трафіку, спостережуване раніше. Однак сама наявність аномалії ще не свідчить про наявність атаки. Для прийняття рішення про наявність загрози необхідний аналіз виявленої аномалії. У випадку повільних DoS-атак, аномалії можуть мати форму короткочасних та невеликих сплесків трафіку, як показано на рисунку 2.6.

При отримані декількох таких піків трафіку з фіксованими інтервалами є показником можливої повільної DoS-атаки. Проте, тривалість одного циклу атаки є досить великою. Очікувати протягом довгого періоду часу, щоб зробити висновок про наявність повільної DoS-атаки, є нераціональним і небезпечним, особливо з урахуванням нормального функціонування системи. Тому є необхідність вибору меншого інтервалу часу для спостереження.

Ще одним видом атак є низькошвидкісні DoS-атаки (LDoS), які часто використовують вразливості програмного забезпечення та дизайну. Наприклад, атака Slowloris названа на честь азійського примата і використовує повільну стратегію. Вона відправляє невеликі фрагменти HTTP-запитів на сервер з певними інтервалами, що призводить до того, що запит не завершується, і сервер очікує його завершення. Це спричиняє накопичення незавершених запитів на сервері, що використовує його ресурси та знижує його продуктивність. Запити Slowloris надсилаються з наміром зайняти доступні з'єднання з сервером, утримуючи їх відкритими, але не закінченими.

Цей вид атаки є особливо небезпечним, оскільки вона може бути успішною при низькій пропускній здатності атакуючого з'єднання, а також не вимагає великого обсягу трафіку. Тим самим, Slowloris може спричинити відмову в обслуговуванні (DoS) навіть на серверах з високою потужністю і широкою смугою пропускання.

Запобігання атакам Slowloris та іншим низькошвидкісним DoS-атакам включає в себе використання захисних механізмів, які можуть відслідковувати та виявляти незавершені з'єднання, обмежувати час очікування на запити та застосовувати стратегії, які дозволяють ефективно управляти ресурсами сервера. Також важливо

регулярно оновлювати серверне програмне забезпечення та виправляти виявлені вразливості, щоб ускладнити успішну реалізацію таких атак.

Slowloris є інструментом атаки, розробленим Робертом Хансеном (відомий як RSnake), який спрямований на зайняття багатьох з'єднань на веб-сервері. Ця загроза працює шляхом відкриття з'єднань на цільовому сервері і відправки неповного запиту. Атака постійно надсилає наступні HTTP-заголовки з інтервалами, але не завершує запити, щоб утримувати ці зв'язки відкритими.

Однак атака не завершує запити для звільнення цих з'єднань, поки сервер не зможе обробити запити від законних клієнтів. Існують інші інструменти та методології, схожі на Slowloris. Деякі з них включають:

- Повільний іонний залп.
- PyLoris;
- QSlowloris (можливий для Windows);

Ion Cannon з низькою орбітою (LOIC) та Ion Cannon з високою орбітою (HOIC) стали популярними інструментами для DDoS-атак для різних хакерських груп, таких як Anonymous чи Syrian Electronic Army. Ці інструменти дозволяють навіть нетехнічним користувачам створювати DDoS-атаки за допомогою своїх власних комп'ютерів замість традиційних бот-мереж.

DDoS-атаки з використанням "нульового дня" (часто називають "вбивцями одного пакета") використовують вразливості в системах, що дозволяють зловмиснику відправити один або кілька пакетів до цільової системи, що призводить до стану DoS (відмови в обслуговуванні) або перезавантаження пристрою. Ці DDoS-атаки з нульовим днем часто є складними для виявлення, оскільки постачальники послуг часто не мають інформації про такі вразливості, і не існує жодних патчів або виправлень, які можна застосувати. Ці атаки використовують уразливості, які ще не відомі розробникам програмного забезпечення або виробникам обладнання, що використовується в системі.

Уразливості та експлойти для таких атак зазвичай продаються на підпільному ринку серед кіберзлочинців, що робить їх однією з найбільш небезпечних загроз для будь-якої організації. Зловмисники можуть використовувати ці уразливості, щоб

спровокувати стан DoS або перезавантажити систему, завдаючи серйозної шкоди функціонуванню та доступності.

Озброєння такими видами атак, як DDoS-атаки з нульовим днем, стає новим стандартом для кіберзлочинців, оскільки вони дозволяють здійснювати широкомасштабні атаки без попереднього попередження або виявлення. Це ставить під загрозу інфраструктуру Інтернету, бізнес-системи та особисті дані користувачів, що робить боротьбу з цими атаками надзвичайно важливою для забезпечення кібербезпеки.

Атаки на рівні протоколів можуть включати форму атаки, відому як SYN-флуд. Під час SYN-флуду зловмисник надсилає на сервер видимо нормальні запити SYN, які призводять до відправки сервером відповідей SYN-ACK (синхронізоване підтвердження). Зазвичай клієнт відповідає на ці відповіді шляхом відправки підтверджуючого запиту ACK, що встановлює з'єднання між клієнтом і сервером. Проте, під час атаки SYN-флуд зловмисник не відправляє остаточний ACK, залишаючи сервер з великою кількістю незавершених запитів SYN-ACK.

Цей метод атаки призводить до того, що на сервері залишається значна кількість незавершених звернень SYN-ACK, які стають непотрібним навантаженням для системи. Таке навантаження може викликати затримки або відмову в обробці дійсних з'єднань, що призводить до зниження продуктивності та доступності сервера [14].

Отже, атаки затоплення SYN на рівні протоколів створюють надмірне навантаження на сервер шляхом надсилання великої кількості незавершених звернень SYN-ACK, що призводить до перевантаження його ресурсів і порушення нормального функціонування.

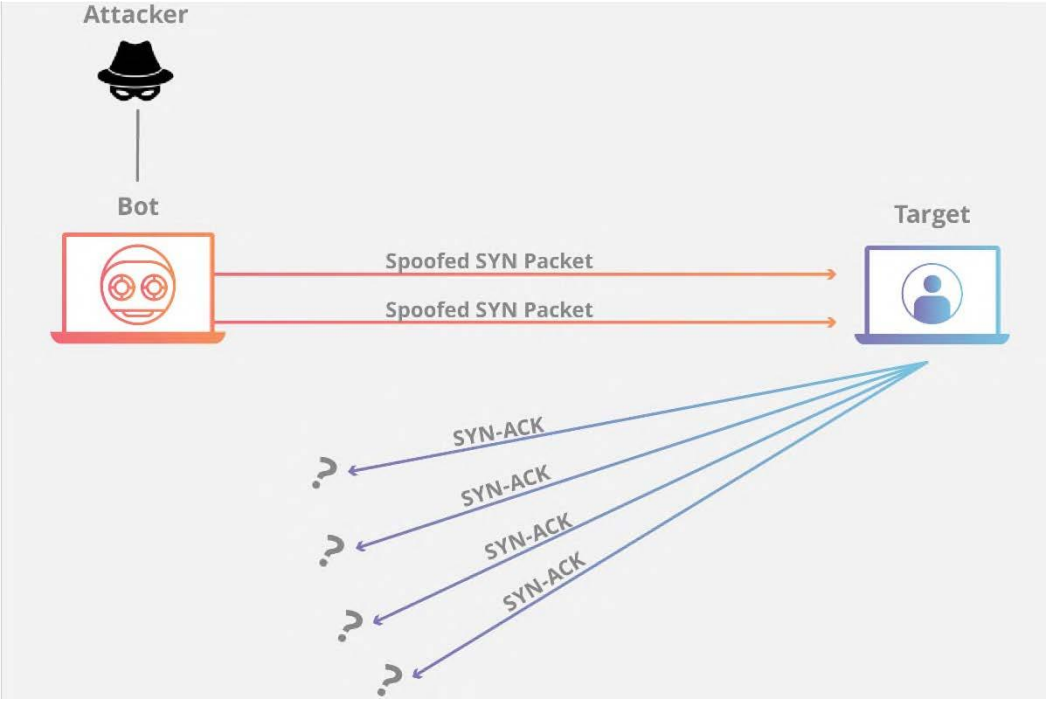


Рис. 2.7 - Протокольні атаки

Атака "Ping of Death" полягає в спробі зламати або зупинити сервер шляхом надсилання звичайного запиту ping, який може бути або фрагментованим, або надмірно великим. Стандартний розмір заголовка IPv4 складає 65 535 байтів. При надсиланні пакету пінг більшого розміру, цільовий сервер фрагментує його. Пізніше, при формуванні відповіді, повторна збірка цього великого пакету може призвести до переповнення буфера і збою системи.

Потокові атаки на протоколи управління Інтернетом, такі як атаки повені через протокол ICMP (Internet Control Message Protocol), існують вже багато років. Вони є одними з найдавніших типів атак DoS і флуд-атак [15]. Під час атак повені ICMP зловмисник перенасичує цільовий ресурс запитами exo (ping) ICMP, великими пакетами ICMP та іншими типами ICMP, що призводить до значного насичення і замедлення мережевої інфраструктури жертви. Цей процес показано на рисунку 2.8.

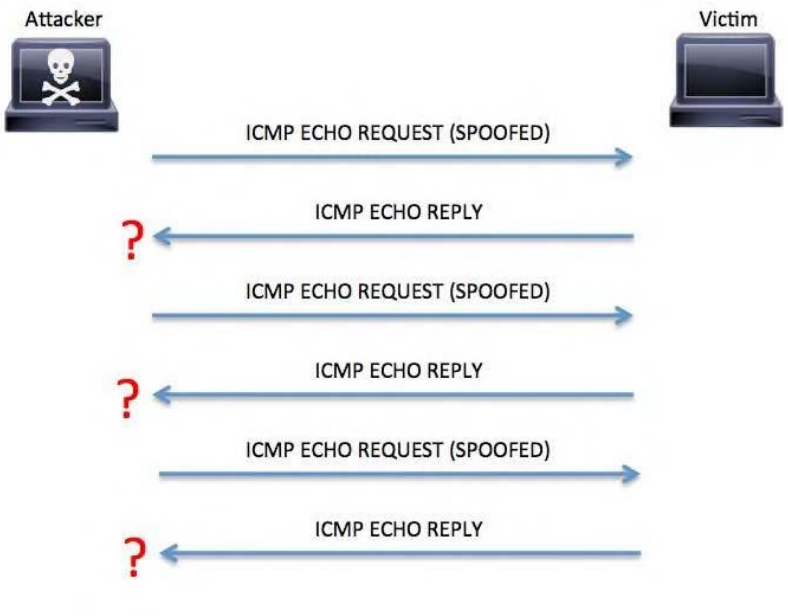


Рис. 2.8 - Приклад повені ICMP

Атака smurf - це ще один тип атаки на основі протоколу ICMP. Назва "smurf" походить від оригінального вихідного коду інструмента експлойту smurf.c, створеного користувачем з псевдонімом TFreak у 1997 році. Під час атаки smurf зловмисник передає велику кількість ICMP-пакетів з підробленими IP-адресами жертви в мережу за допомогою IP-адреси трансляції. Це змушує пристрої в мережі реагувати, надсилаючи відповідь на вихідну IP-адресу, що стає жертвою атаки. Цей обмін показано на рисунку 2.9.

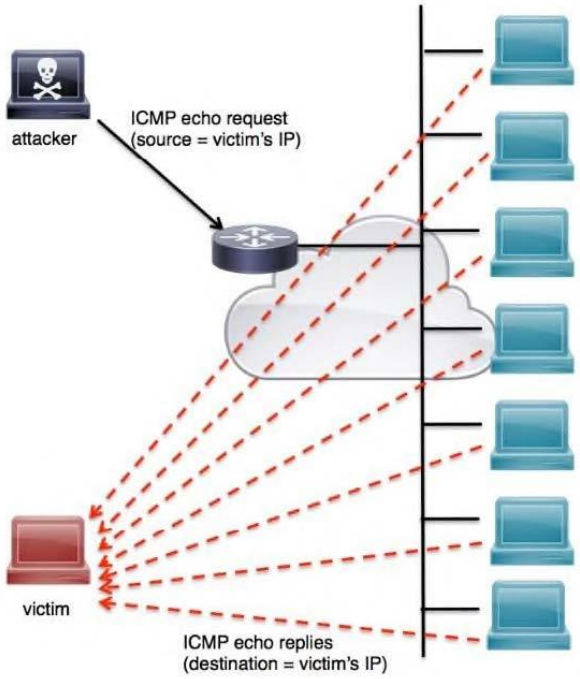


Рис. 2.9 - Смурф атака

Існує простий спосіб зменшити вплив цієї атаки на пристроях Cisco IOS, застосовуючи команду "no ip directed-broadcast" на підінтерфейсі, як показано у наступному прикладі:

- Маршрутизатор (конфігурація-якщо) # немає ip directed-broadcast;
- Маршрутизатор (конфігурація) # інтерфейс GigabitEthernet 0;
- SYN flood атаки.

Під час, коли клієнт (хост) починає TCP-з'єднання з сервером, клієнт і сервер взаємодіють за допомогою послідовності повідомлень для встановлення з'єднання. Цей процес відомий як TCP three-way handshake (тристороннє рукостискання TCP). Цей процес показано на рисунку 2.10.

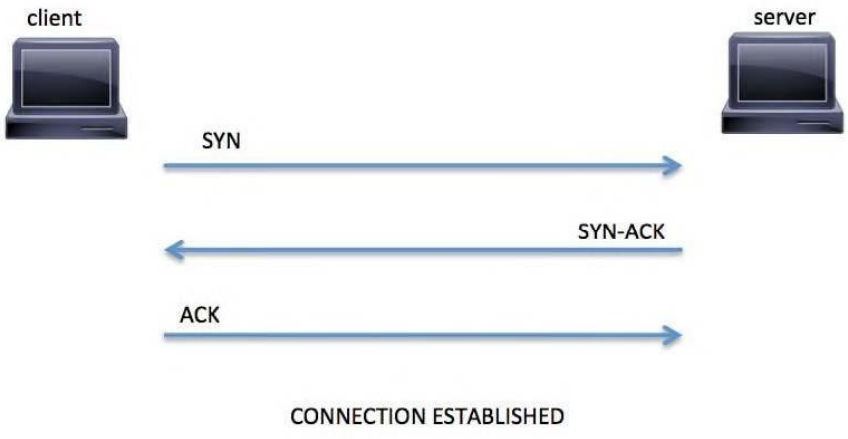


Рис. 2.10 - Тристороннє рукостискання TCP

• Сервер підтверджує цей запит, відправляючи клієнту повідомлення SYN-ACK.

• Клієнт ініціює з'єднання, відправляючи серверу повідомлення SYN (синхронізація).

• Клієнт відповідає ACK (підтвердженням), встановлюючи зв'язок.

Атаки потоку UDP. Подібно до атак потоку TCP, головною метою зловмисника при здійсненні атаки потоку UDP є виклик голодування системних ресурсів. Атака потоку UDP полягає в надсиланні великої кількості UDP-пакетів на випадкові порти системи жертви. Система помітить, що жодна програма не слухає цей порт і не відповідає пакетом "Призначення недоступне" ICMP. Пізніше, якщо надсилається велика кількість пакетів UDP, жертва буде змушена відправити багато пакетів ICMP. У більшості випадків такі атаки здійснюються шляхом підробки IP-адреси зловмисника. Більшість сучасних операційних систем обмежують швидкість відповідей ICMP, що зменшує вплив і трохи послаблює такий тип DDoS-атаки.

Краплеві атаки. Атаки сльози полягають у надсиланні спеціально сформованих пакетів з великими корисними навантаженнями на систему жертви. Сучасні операційні системи, навіть зараз, не повністю захищені від цього типу атак, але через відсутність фрагментації TCP та повторну збірку в старій реалізації операційних систем, цей тип атак може призвести до збоїв у таких системах.

Підсумовуючи розглянуті типи DDoS-атак, запропоновано класифікацію за такими критеріями (рис. 2.11).

Рис 2.11 Класифікація DDoS-атак

За кількістю задіяних пристроїв - за цією ознакою атаку можна класифікувати на наступні категорії: прості DoS-атаки; групові DDoS-атаки - за допомогою невеликої кількості добровільно задіяних комп'ютерів (до 99 пристроїв); та масові DDoS-атаки - залучають понад 100 пристроїв.

Відповідно, необхідно розрізняти методи боротьби з цими типами атак. У випадку простих або групових атак можна вручну блокувати пакети з відповідних машин, використовуючи чорний список. Однак, у випадку масових атак, блокування всіх можливих джерел атак вручну стає досить проблематичним завданням, особливо при ідентифікації законних користувачів від зловмисників.

Залежно від джерела атаки, можна класифікувати напади на зловмисників наступним чином: волевиявлені атаки безпосередньо з машин зловмисників; атаки з використанням ботнетів; загрози, що використовують фізичні і віртуальні виділені сервери; атаки з використанням проміжних машин і інструментів тунелювання; а також атаки з використанням випадкових користувачів.

Потрібно відзначити, що в разі здійснення атаки з використанням виділених серверів, навіть невелика кількість пристроїв може спричинити значний обсяг трафіку, оскільки такі сервери зазвичай мають мультигігабітні канали. При застосуванні захисту від таких атак за допомогою проміжних машин і інструментів тунелювання важливо враховувати, що визначити, чи використовується даний інструмент тунелювання для атаки чи для законного доступу до служби, може бути складно, оскільки один і той самий інструмент може мати обидва використання. Встановлення цієї різниці може становити значні труднощі.

2.3 Архітектура DDoS-атак за їх видами

Атаки з використанням бот-мереж можна класифікувати за типом використаних машин, таких як мобільні пристрої, інфіковані сервери і домашні комп'ютери. Щодо кількості атакуючих пристроїв, DDoS-атаки можуть бути статичними (з фіксованою кількістю пристроїв), з динамічним керуванням (кількість і розташування атакуючих пристроїв можуть змінюватися з часом, існує формальний список джерел нападу, такі як користувачі каналів IRC, вузли Tor, список IP-адрес), або динамічними без контролю - коли немає технічної можливості створити список атакуючих машин.

Атаки можна класифікувати за способом управління, включаючи керовані атаки (з віддаленим керуванням нападом), ручні атаки (зловмисник вручну відправляє пакети) і автоматичні атаки (атака виконується без безпосереднього втручання людини).

Залежно від засобів управління атакою, можна виділити засоби зв'язку для прямого управління (централізоване управління, де пристрої мають відкритий порт

для ідентифікації вихідних машин) і засоби непрямого керування (машини не мають відкритого порту і керуються за допомогою зворотних з'єднань чи додаткових протоколів).

Атаки, які використовують бот-мережі, можна поділити залежно від типу мережного підключення, на такі категорії: випадкове сканування, сканування по списку і зворотній зв'язок. Випадкове сканування означає, що нападник випадково сканує IP-адреси для пошуку інфікованих машин. Сканування по списку включає нападника, який має список інфікованих машин. Зворотній зв'язок означає, що інфіковані машини таємно повідомляють нападника про своє зараження.

Атаки можна також класифікувати за вразливістю. Семантичні атаки використовують певні служби або протоколи, тоді як "паводкові" атаки спрямовані на спробу "дурного" перевантаження шляхом великого розміру пакетів або їх великої кількості.

Щодо правильності вихідної адреси атаки, їх можна поділити на атаки з правильним джерелом, де джерело атаки чітко визначено в пакеті даних, атаки з підробленим джерелом, де адреса джерела відсутня або вказана некоректно, і зворотні атаки, коли атака здається виконуватися легальною службою, яка фактично відповідає на неправильно сформовані запити (наприклад, DNS або Google).

Атаки можна класифікувати за силою нападу. Це включає атаки з постійною силою, коли атака виконується з фіксованою силою, випадковою потужністю, коли сила змінюється хаотично, певною змінною силою, коли потужність змінюється за відомим алгоритмом, атаки з коливальною силою, коли сила атаки коливається або пульсує, а також атаки зі збільшенням потужності, коли сила атаки постійно зростає.

Щодо рівня реалізації нападу, атаки можна класифікувати наступним чином: атаки на фізичному рівні, які включають фізичні перешкоди в комп'ютерній системі, такі як обрив кабелю, підвищення напруги або випромінювання; атаки на рівні каналу, які спрямовані на атаку на фізичному рівні мережних каналів; атаки на мережному рівні, які впливають на IP-пакети; атаки на транспортному рівні, які спрямовані на рівні сегментів та дейтаграм; атаки на рівні сесії, які здійснюються в

межах логічних з'єднань; атаки на рівні програми, які використовують протоколи на прикладному рівні; та атаки на рівні сервісу, які використовують особливості певної програми чи послуги.

Таким чином, атаки можуть бути класифіковані за різними критеріями, включаючи тип мережного підключення, вразливість, правильність вихідної адреси, силу нападу та рівень реалізації.

Очевидно, що вищий рівень атаки має більший вплив на рівень обслуговування. Таким чином, атака на фізичному або мережному рівні може призвести до відмови всієї корпоративної мережі, атака на рівні програми може призвести до недоступності веб-сервера та всіх розміщених на ньому веб-ресурсів, тоді як атака на рівні служби може обмежити доступ лише до певної послуги, наприклад, до конкретного веб-ресурсу.

Залежно від впливу на жертву, атаки можуть бути класифіковані на такі типи: блокуючі атаки, які призводять до блокування доступу, що в результаті може призвести до втрати ділових зв'язків з клієнтами; атаки, що збільшують споживання ресурсів, які не повністю блокують доступ, але значно збільшують навантаження на ресурси; атаки, які призводять до знищення, такі атаки руйнують компоненти системи, призводячи до втрати даних через переповнення жорсткого диска, перегрів чи несправність обладнання.

Блокуючі атаки можуть бути поділені на напади з можливістю відновлення, коли після припинення атаки можливе відновлення з'єднання з клієнтом, та напади без можливості відновлення, коли після припинення атаки з'єднання з клієнтом не може бути відновлене без втручання вручну. За типом атаки на вразливість можна класифікувати на напади на протокол та напади на реалізацію.

2.4 Життєвий цикл DDoS-атаки

Протягом останнього десятиліття мотиви, цілі та масштаби DDoS-атак зазнали змін. Однак основна ціль атаки - обмежити доступ користувачів до мережевих ресурсів - залишається незмінною. Компоненти, які складають такі атаки, також

майже не змінилися. Для кращого розуміння життєвого циклу DDoS важливо спочатку зрозуміти компоненти, які утворюють інфраструктуру таких атак. Описаний тут життєвий цикл зосереджений переважно на ботнетах або колекціях зомбі-машин, які отримують команди від одного або декількох серверів для адміністративного управління.

Перший етап - розвідка. Початок DDoS-атаки включає ручні або автоматизовані спроби знайти вразливі хости, які можуть виступати як сервери командно-контрольного центру (C2) або клієнти ботнетів. Розвідка може бути здійснена зловмисником у формі IP-зондів (часто називають їх пінг-розгортками). Ці зонди можуть створити менший список хостів для подальшого зондування шляхом сканування портів. Сканування портів надає більше інформації про хост, наприклад, послуги, які він пропонує, та версію операційної системи. Зловмисник використовує цю інформацію для визначення найпростішого способу використання вразливості.

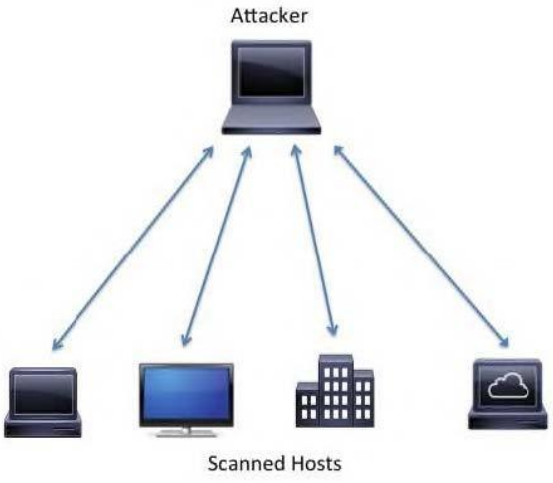


Рис. 2.12 - Розвідка DDoS

Після виявлення потенційних жертв, зловмисники спрямовують свої зусилля на використання та розширення цих систем, з метою отримання контролю над ними. Після успішної експлуатації система може бути використана як складова інфраструктури для проведення DDoS-атак. Залежно від потреб зловмисника,

скомпрометований пристрій може виконувати функції сервера для відправки DDoS-трафіку або розповсюджувати експлойти на інші пристрої. З часом ботнет може зростати до великої кількості хостів, від кількох тисяч до навіть мільйонів.

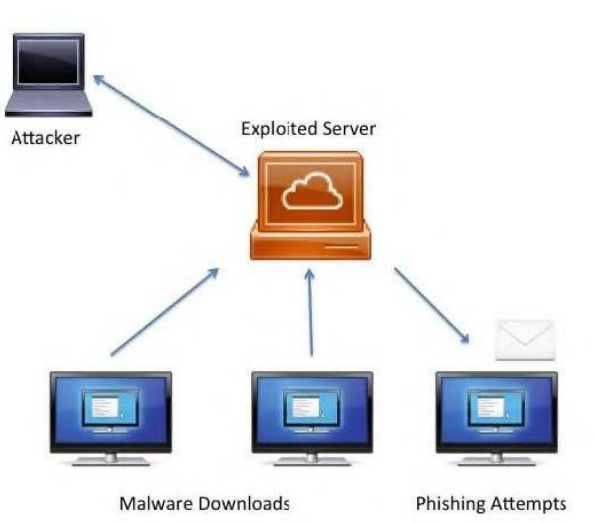


Рис. 2.13 - Компоненти інфраструктури DDoS

Потрібно відзначити, що не всі хости, що беруть участь в DDoS-атаках, є експлуатованими жертвами. Іноді користувачі, які підтримують певну політичну справу, свідомо встановлюють програмне забезпечення DDoS з метою завдати шкоди конкретній цілі. Крім того, бот-мережі можуть використовуватись для інших цілей, не пов'язаних з DDoS-атаками.

Командування та управління. Ботнети потребують певного рівня обслуговування. Один із загально використовуваних протоколів комунікації ботнету є Internet Relay Chat (IRC), що базується на моделі клієнт/сервер. Зомбі-пристрої та сервери взаємодіють, щоб надсилати клієнтам команди, наприклад, налаштування тривалості атаки або оновлення шкідливого програмного забезпечення. Використання моделі одноранговогo зв'язку (P2P) ускладнює виявлення та обмеження ботнету, оскільки з'єднання здійснюються безпосередньо між багатьма пристроями, зменшуючи ризик відключення від центрального сервера.

Тестування. Коли ботнет досягає критичної маси, що дозволяє генерувати достатньо трафіку для насичення жертви, часто відбувається період тестування. Під час цього тестування потенційні жертви спостерігають значний обсяг трафіку протягом декількох секунд або хвилин. Зловмисник оцінює ефективність атаки та вносить корективи для створення стійкого нападу. Трафік часто змінюється протягом тривалої атаки, і зловмисник аналізує ці зміни, щоб максимізувати вплив на жертву.

Стійкий напад. Правопорушник вирішує, коли наказати клієнтам ботнету розпочати надсилання трафіку до цільової інфраструктури. Основна фаза DDoS-атаки може тривати від годин до тижнів, залежно від мотивів зловмисника. Атаки на рівні 7 (такі як HTTP GET або POST-атаки) стають все більш популярними. Підсилення атаки може посилювати її вплив.

2.5 Принципи основних методів боротьби проти DDoS-атак

До існуючих методів захисту від DDoS-атак можна віднести наступні:

1. Виявлення та блокування атак за допомогою спеціального програмного забезпечення (наприклад, програмних інструментів, що визначають трафік, який генерується ботнетом).
2. Застосування мережевих пристроїв, що здатні розпізнавати та фільтрувати трафік, що спрямований на атаку.
3. Використання технологій захисту від DDoS на рівні провайдера

DPI (глибинний інспектор пакетів) є технологією, що дозволяє аналізувати пакети даних, що передаються через мережу, та розпізнавати конкретні протоколи, додатки або віруси. DPI може бути застосований для виявлення та блокування атак DDoS, оскільки він здатен розпізнавати аномальний трафік, що спричинений атакою.

ВИСНОВКИ ДО РОЗДІЛУ 2

У процесі виконання роботи було розглянуто основні етапи життєвого циклу атаки, такі як розвідка, експлуатація та розширення, командування та управління, тестування та стійкий напад. Основна мета DDoS-атаки полягає у забороні доступу користувачів до ресурсів, хоча мотиви та цілі таких атак можуть змінюватися. DDoS атака здатна знищити великі веб-сервіси, для яких зазвичай потрібні тисячі скомпрометованих машин. Структура такої розподіленої атаки є складною. Для реалізації атаки формується ботнет або мережа зомбі-машин, які використовуються для надсилання трафіку до жертви атаки. Описані компоненти інфраструктури атаки включають розвідку, експлуатацію та розширення ботнету, командування та управління через протоколи, такі як IRC або P2P, тестування ефективності атаки та нарешті, стійкий напад. Даний аналіз допоміг зрозуміти ключові аспекти DDoS-атак та їхній життєвий цикл.

……

РОЗДІЛ 3
АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ МУЛЬТИМЕДІЙНОГО СЕРЕДОВИЩА ВІД DDOS-АТАК ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ DPI

3.1. Структура та архітектура технології DPI

Технологія DPI може бути використана для розробки архітектури системи захисту від DDoS-атак. *Процес розробки такої системи може включати наступні етапи*:

1. Аналіз вимог: на цьому етапі проводиться визначення вимог до системи захисту. Це включає вимоги до швидкості обробки трафіку, точності виявлення атак і інших параметрів.

2. Проектування архітектури: на цьому етапі створюється архітектура системи захисту, використовуючи DPI. Це включає визначення компонентів системи, таких як мережеві пристрої, сервери, програмне забезпечення тощо.

3. Вибір технологій: на цьому етапі обираються технології, які будуть використовуватися для реалізації системи захисту на основі DPI. Це може включати вибір мережевих пристроїв з підтримкою DPI, програмного забезпечення для аналізу трафіку тощо.

4. Розробка та тестування системи: на цьому етапі розробляється система захисту на основі DPI, і проводяться тестування для перевірки її працездатності та ефективності.

5. Впровадження системи: на цьому етапі система захисту на основі DPI встановлюється в мультимедійну мережу і налагоджується для забезпечення захисту від атак DDoS.

Основними компонентами архітектури системи захисту на основі DPI можуть бути:

1. DPI-пристрої: мережеві пристрої з підтримкою DPI, що відповідають за аналіз трафіку.

2. Алгоритми машинного навчання: використовуються для виявлення аномального трафіку та атак DDoS.

3. Система керування політикою безпеки дозволяє налагоджувати правила фільтрації трафіку та контролювати доступ до мережевих ресурсів. Вона забезпечує можливість конфігурування параметрів системи захисту, встановлення правил для блокування атак та аномального трафіку, а також управління іншими аспектами безпеки мережі.

4. Система моніторингу: вона відповідає за виявлення підозрілого трафіку та постійне спостереження за станом мережі. Ця система здійснює постійний аналіз мережевого трафіку, спостерігає за потенційними загрозами та генерує сповіщення про події, що можуть вказувати на атаку.

5. Система логування та аудиту: вона відповідає за збір та аналіз логів трафіку з метою виявлення аномалій та атак. Ця система реєструє всі події, пов'язані з мережевим трафіком, зберігає їх у вигляді логів і забезпечує можливість подальшого аналізу для виявлення потенційних загроз.

6. Система автоматичного реагування: ця система відповідає за швидке виявлення та блокування атак DDoS. Вона заснована на алгоритмах, які автоматично розпізнають атаки та приймають відповідні заходи для їх припинення, наприклад, блокування підозрілого трафіку або встановлення обмежень на певних рівнях мережі.

7. Система резервного копіювання: ця система забезпечує зберігання резервних копій даних та налаштувань системи захисту. Вона гарантує, що в разі виникнення непередбачених ситуацій або випадкового втрати даних, можна відновити систему захисту до попереднього стану шляхом використання збережених резервних копій. Система резервного копіювання забезпечує регулярне створення резервних копій і їх зберігання на надійних пристроях або віддалених серверах. Це забезпечує високу надійність і готовність системи захисту до відновлення після будь-яких небезпечних подій чи втрати даних.

Ці компоненти разом утворюють архітектуру системи захисту на основі DPI, яка забезпечує виявлення, блокування та відповідь на DDoS-атаки. Перефразований текст:

Розробка архітектури системи захисту від DDoS-атак на основі технології DPI може включати наступні етапи: аналіз вимог, проектування архітектури, вибір технологій, розробка та тестування системи, та впровадження системи. Основними компонентами архітектури є DPI-пристрої, алгоритми машинного навчання, система керування політикою безпеки, система моніторингу, система логування та аудиту, система автоматичного реагування і система резервного копіювання. Використання цих компонентів дозволяє ефективно виявляти, блокувати та відповідати на DDoS-атаки, забезпечуючи безпеку мережі.

3.2. Класифікація засобів моніторингу та аналізу

Інструменти, які пропонують для моніторингу та аналізу обчислювальних мереж, можна розділити на кілька груп:

Системи управління мережею (Network Management Systems) - централізовані програмні системи, які збирають дані про стан мережевих пристроїв та інформацію про трафік у мережі. Функціонал цих програм не обмежений моніторингом і аналізом мережі. Додатково, в напівавтоматичному або автоматичному (залежно від реалізації) режимі, здійснюються дії з управління мережею: налаштування і зміна адресних таблиць комутаторів та іншого обладнання, увімкнення та вимкнення портів пристроїв. До систем у цій категорії належать HPOpenView, SunNetManager, IBMNetView.

Вбудовані системи діагностики та управління (Embedded systems). Системи цього типу виконані у вигляді програмно-апаратних модулів, які встановлюються в комунікаційне обладнання, або - в операційну систему у вигляді програмних модулів. Вони дають змогу керувати і діагностувати тільки тим пристроєм, на якому знаходяться. Прикладом таких систем є модуль управління концентратором Distributed 5000, який виконує функції автосегментації портів після виявлення несправностей, приписування портів внутрішнім сегментам концентратора і деякі інші. Зазвичай, вбудовані модулі управління також виконують роль SNMP-агентів, передаючи дані про стан пристрою в систему управління.

Засоби управління системою (System Management). Інструменти з цієї групи виконують функції, аналогічні функціям систем управління, але стосовно інших об'єктів. У першому випадку об'єктом управління є програмне та апаратне забезпечення комп'ютерів мережі, а в другому - комунікаційне обладнання. При цьому частина функцій цих двох видів систем можуть дублюватися (наприклад, засоби управління системою можуть проводити найпростіший аналіз трафіку).

Аналізатори протоколів (Protocol analyzers) - це програмні або апаратно-програмні системи, які використовуються тільки для моніторингу та аналізу трафіку в мережах. Хорошим аналізатором вважається той, який може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах - приблизно кількох десятків. Ця група систем може встановлювати деякі логічні умови для захоплення окремих пакетів і виконувати повне декодування пакетів, тобто відображати в зручній для користувача формі вкладеність пакетів протоколів різних рівнів із розшифруванням змісту кожного поля пакета. Коли починають проєктувати або модернізувати мережу, часто виникає потреба в кількісному вимірі характеристик мережі: наприклад, затримки, що виникають на різних етапах, частота виникнення вибіркових подій, інтенсивність потоків даних лініями зв'язку, час реакції на запити.

Обладнання для діагностики та сертифікації кабельних систем. З назви стає зрозумілим призначення цієї групи. Умовно можна виділити чотири підтипи подібного обладнання: кабельні сканери, мережеві монітори, мультиметри та прилади для сертифікації кабельних систем.

Експертні системи з'єднують людські знання про виявлення причин аномальної роботи мереж і можливих способів повернення мережі в робочий стан. Найчастіше вони представлені у вигляді окремих підсистем інших засобів моніторингу та аналізу мереж, розглянутих раніше.

До простого варіанту експертної системи належить контекстно-залежна help-система, а більш складні являють собою так звані бази знань, які мають елементи штучного інтелекту. Прикладом цієї групи є система, вбудована в систему управління Spectrum компанії Cabletron.

Багатофункціональні пристрої аналізу та діагностики. Через широке поширення локальних мереж з'явилася потреба в розробці недорогих портативних приладів із функціоналом кількох пристроїв: кабельних сканерів, програм мережевого управління та аналізаторів протоколів. Як приклад можна навести Compas компанії MicrotestInc або 675 LANMeter компанії FlukeCorp.

Також варто відзначити ще два способи моніторингу мережі.

- *Перший* - це маршрутизаторо-орієнтований. Він являє собою моніторинг, вбудований безпосередньо в маршрутизатор, який не потребує додаткового встановлення іншого забезпечення.
- *Другий спосіб*, відповідно, - це не орієнтований на маршрутизатори, тобто це підібране самим фахівцем необхідне апаратне і програмне забезпечення для поточних потреб.

3.3. Системи виявлення та запобігання вторгненням

Впровадження подібних систем для захисту інформації є необхідністю для всіх серйозних мережевих інфраструктур, оскільки існують програми, які постійно вишукують уразливості в будь-якому обладнанні, підключеному до глобальної мережі. Наприклад, пошуковий движок Shodan в автоматичному режимі збирає інформацію про під'єднані пристрої, які не мають жодної частини системи безпеки. Користувачі Shodan знаходять системи управління крематорієм, газовою станцією тощо, які не мають реквізитів доступу, або вони налаштовані за замовчуванням. Отже, до них можна легко проникнути та зменшити працездатність.

Проти такого впливу і спрямовані системи виявлення та запобігання вторгненням, тому вони є часто використовуваним інструментом у політиці безпеки.

Система виявлення вторгнень (СВВ) (англ. Intrusion Detection System (IDS)) - програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу.

Система запобігання вторгненням (СЗВ) (англ. Intrusion Prevention System (IPS)) - програмний або апаратний засіб, що здійснює моніторинг мережі або системи в реальному часі з метою виявлення, запобігання або блокування шкідливої активності.

Системи запобігання вторгненням можна вважати розширенням систем виявлення вторгнень, оскільки завдання відстеження атак залишається однаковим. Але СЗВ повинна відстежувати вторгнення в реальному часі й одразу здійснювати дії щодо запобігання атакам. Для цього вони використовують: скидання з'єднань, блокування потоків трафіку в мережі, видачу сигналів оператору. Крім цього, такі системи можуть дефрагментувати пакети, змінювати порядок TCP пакетів для захисту від пакетів зі зміненими SEQ і ACK номерами тощо.

Ці системи використовуються для автоматизації процесу контролю над подіями, які протікають у комп'ютерній системі або мережі, та аналізу цих подій з метою пошуку ознак проблем безпеки. Через те, що кількість різних способів і видів організації несанкціонованих вторгнень у мережі за останній час значно збільшилась, то системи виявлення вторгнень стали обов'язковою частиною інфраструктури безпеки для більшості організацій. Цьому сприяють як велика кількість літератури з цього питання, яку потенційні зловмисники уважно вивчають, так і все більш витончені підходи до виявлення спроб проникнення в інформаційні системи.

Сучасні системи виявлення вторгнень мають різну архітектуру, основними з яких є: мережева та локальна. Мережеві системи встановлюють на виділених для цих цілей комп'ютерах так, щоб вони могли аналізувати трафік, що протікає локальною обчислювальною мережею. Локальні ж системи розміщуються на тих комп'ютерах, які потребують захисту, і вивчають певні події (програмні виклики або дії користувача).

Крім архітектури СВВ також можуть розрізняти за методикою виявлення: частина систем шукає аномальну поведінку, інша - зловмисну.

3.4. Методики виявлення аномальної та зловмисної поведінки користувачів

Системи виявлення аномальної поведінки (від англ. Anomaly Detection) засновані на тому, що СВВ відомі ознаки, що характеризують правильну або допустиму поведінку об'єкта спостереження. Під "нормальною" або "правильною" поведінкою розуміють дії, які виконуються об'єктом і не суперечать політиці безпеки.

Системи виявлення зловмисної поведінки (Misuse Detection) засновані на тому, що заздалегідь відомі ознаки, що характеризують поведінку зловмисника. Найпоширенішою реалізацією технології виявлення зловмисної поведінки є експертні системи (наприклад, системи Snort, RealSecure IDS, Enterasys Advanced Dragon IDS).

Розглянемо детальніше технології, що використовуються в цих системах (рисунок 3.1).

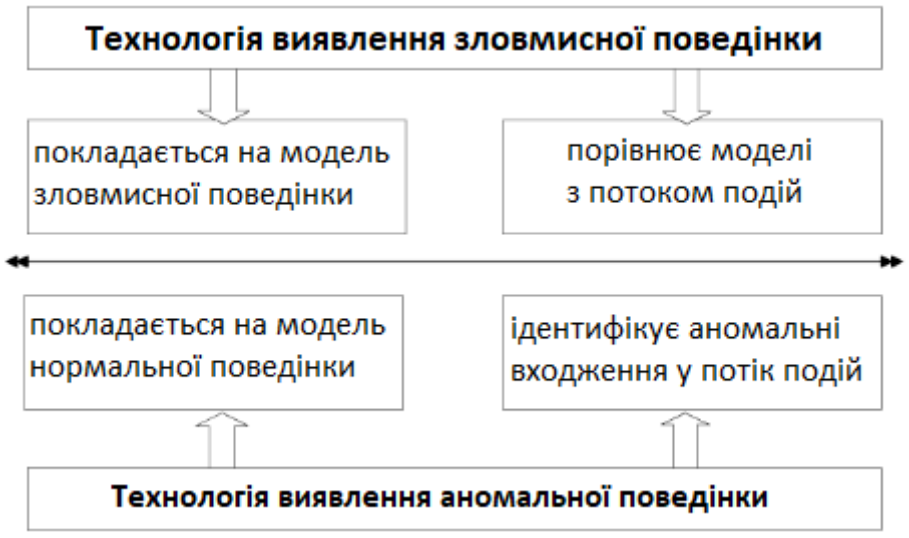


Рис. 3.1 Існуючі технології СВВ

3.5. Технології виявлення аномальної діяльності

Для захисту мультимедійної мережі від атак DDoS за допомогою технології DPI можна використовувати такі підходи:

1. Виявлення та блокування трафіку з високою інтенсивністю: Використовуючи DPI, можна розпізнати трафік з високою інтенсивністю, що є характерним для атак DDoS, та ефективно його блокувати.

2. Використання алгоритмів машинного навчання для виявлення атак: DPI може бути поєднаний з алгоритмами машинного навчання, що дозволяє виявити аномальний трафік, характерний для атак DDoS, та прийняти відповідні заходи для їх виявлення.

3. Фільтрація трафіку: DPI може бути використаний для фільтрації трафіку на основі конкретних протоколів або додатків, що дозволяє виявити та блокувати небажаний трафік, що є важливим для запобігання атакам DDoS.

4. Застосування технології DPI для захисту мультимедійної мережі від атак DDoS забезпечує ефективний рівень захисту, оскільки DPI може аналізувати трафік на глибинному рівні та розпізнавати аномальний трафік, що є характерним для атак DDoS. Це дозволяє вчасно виявляти та блокувати потенційні загрози, забезпечуючи безпеку мережі.

Датчики-сенсори аномалій ідентифікують незвичайну поведінку, так звані аномалії, у функціонуванні окремого об'єкта. Тому головна складність у застосуванні їх на практиці пов'язана з нестабільністю самих об'єктів, що захищаються, а також зовнішніх об'єктів, що взаємодіють із ними. Об'єктом спостереження може бути мережа загалом, окремий комп'ютер, мережева служба (наприклад, файловий сервер FTP), користувач і так далі Датчики спрацьовують за умови, що напади відрізняються від "звичайної" (законної) діяльності. Тут варто зазначити, що в різних реалізаціях своє визначення допустимого відхилення для спостережуваної поведінки від дозволеної і своє визначення для "порога спрацьовування" сенсора спостереження.

Заходи і методи, які зазвичай використовують у виявленні аномалії, містять такі:

- порогові значення: спостереження за об'єктом виражаються у вигляді числових інтервалів. Вихід за межі цих інтервалів вважається аномальною поведінкою. Параметрами, що спостерігаються, можуть бути, наприклад: кількість файлів, до яких звертається користувач у даний період часу, кількість невдалих спроб входу в систему, завантаження центрального процесора тощо. Пороги можуть бути статичними та динамічними (тобто змінюватися, підлаштовуючись під конкретну систему);

- параметричні: для виявлення атак будується спеціальний "профіль нормальної системи" на основі шаблонів (тобто деякої політики, якої зазвичай має дотримуватися цей об'єкт);

- непараметричні: профіль будується на основі спостереження за об'єктом у період навчання;

- статистичні заходи: рішення про наявність атаки приймається за великою кількістю зібраних даних шляхом їхньої статистичної попередньої обробки;

- заходи на основі правил (сигнатур): вони дуже схожі на непараметричні статистичні заходи. У період навчання складається уявлення про нормальну поведінку об'єкта, яке записується у вигляді спеціальних "правил". Виходять сигнатури "хорошої" поведінки об'єкта;

- інші заходи: нейронні мережі, генетичні алгоритми, що дають змогу класифікувати деякий набір видимих сенсору-датчику ознак.

У сучасних системах виявлення аномалій переважно використовують перші два методи. Слід зауважити, що існують дві крайності під час використання цієї технології:

- виявлення аномальної поведінки, яка не є атакою, і віднесення її до класу атак (помилка другого роду);

- пропуск атаки, яка не підпадає під визначення аномальної поведінки (помилка першого роду). Цей випадок набагато небезпечніший, ніж помилкове зарахування аномальної поведінки до класу атак.

Тому під час встановлення та експлуатації систем такої категорії звичайні користувачі та фахівці стикаються з двома досить нетривіальними завданнями:

- визначення граничних значень характеристик поведінки суб'єкта для зниження ймовірності появи одного з двох вищеописаних крайніх випадків;

- побудова профілю об'єкта - це важко формалізоване і витратне за часом завдання, що вимагає від фахівця безпеки великої попередньої роботи, високої кваліфікації та досвіду.

Як правило, системи виявлення аномальної активності використовують журнали реєстрації та поточну діяльність користувача як джерело даних для аналізу. До переваг систем виявлення атак на основі технології виявлення аномальної поведінки можна віднести те, що вони:

- не потребують оновлення сигнатур і правил виявлення атак;

- здатні виявляти нові типи атак, сигнатури для яких ще не розроблені;

- генерують інформацію, яка може бути використана в системах виявлення зловмисної поведінки.

Недоліками цих систем є таке:

- генерують багато помилок другого роду;

- вимагають тривалого і якісного навчання;

- зазвичай занадто повільні в роботі та потребують великої кількості обчислювальних ресурсів.

3.6. Механізм виявлення та відпрацювання основних етапів захисту від атак

Реалізація розробленої системи захисту на основі DPI може бути проведена за допомогою наступних етапів:

1. Придбання та налаштування необхідного обладнання DPI.
2. Розробка та налаштування правил фільтрації трафіку на основі аналізу аномального трафіку та атак DDoS.
3. Розробка та налаштування алгоритмів машинного навчання для виявлення аномалій трафіку та атак DDoS.

4. Розробка та налаштування системи керування політикою безпеки для налаштування параметрів захисту та контролю над мережевим ресурсами.

5. Розробка та налаштування систем моніторингу, логування та аудиту для виявлення аномалій трафіку та атак DDoS та аналізу логів для виявлення і попередження подібних атак у майбутньому.

6. Розробка та налаштування системи автоматичного реагування на атаки DDoS, включаючи блокування підозрілого трафіку та встановлення додаткових захисних бар'єрів для запобігання майбутнім атакам.

Для обрахунку ефективності системи захисту на основі DPI, можна використовувати тестові середовища для відтворення атак та вимірювання метрик. Такі тестові середовища можуть бути створені шляхом імітації атак DDoS на тестових серверах та мережах. Для збору статистики та аналізу результатів можуть використовуватися спеціальні програмні засоби для моніторингу трафіку та аналізу логів.

Ефективність системи захисту на основі DPI може бути оцінена за допомогою наступних метрик:

1. Виявлення атак: ефективність системи виявлення атак DDoS, виміряна у відсотках.

2. Блокування атак: ефективність системи блокування атак DDoS, виміряна у відсотках.

3. Пропускна здатність: ефективність системи у збереженні пропускної здатності мережі при використанні DPI.

4. Час відклику: час, необхідний системі для виявлення та блокування атак DDoS.

5. Стійкість: здатність системи працювати при великих навантаженнях та під час атак.

Після проведення тестів ефективність системи захисту на основі DPI можна порівняти з іншими методами захисту та визначити її конкурентоспроможність. Для підвищення ефективності системи можна застосовувати методи оптимізації правил фільтрації та алгоритмів машинного навчання, а також використовувати розподілену архітектуру для забезпечення більшої стійкості та пропускної здатності.

3.7. Гнучке балансування анамального трафіку

Балансування навантаження - це метод масштабування ємності, який широко використовується в комп'ютерних мережах. Протоколи маршрутизації обчислюють однакову метрику на кількох шляхах одночасно. Для досягнення ефективності та мінімальної затримки, пристрої балансування навантаження розміщуються на шляху трафіку. Зазвичай використовуються методи, що базуються на хеш-функціях, де вхідний трафік аналізується для виділення ключових частин заголовка пакета, і пакети розподіляються між кількома виходами. Ефективність алгоритму залежить від статистичних характеристик трафіку та відповідного алгоритму. Більшість потоків у мережевому трафіку є короткочасними і не вносять суттєвого внеску в загальний обсяг трафіку (понад 80% потоків тривають менше 10 секунд). Однак існує невеликий відсоток довготривалих потоків, які становлять значну частку в загальному обсязі. Наявність таких довготривалих потоків становить виклик для рівномірного розподілу трафіку по кільком шляхам, оскільки будь-який хеш-алгоритм важко розділити такий потік на паралельні шляхи або збалансувати його пропускну здатність з іншими потоками, що передаються по альтернативних шляхах.

У процесі опрацювання та зберігання інформації неминуче виникає необхідність в обміні даними між учасниками цього процесу. З кінця 70-х років почався бурхливий розвиток комп'ютерних мереж і супутнього мережевого обладнання. Локальні та глобальні мережі продовжують розвиватися, виникають нові протоколи передавання даних, розширюються апаратні можливості мережевого устаткування, зростає кількість підключених абонентів і сумарний обсяг трафіку.

Такий інтенсивний розвиток галузі тягне за собою низку проблем. Одна з них полягає в тому, що при зростаючій кількості споживачів інформаційних послуг збільшуються вимоги до мережевого і серверного обладнання, яке використовується для підтримки належного рівня якості обслуговування. Друга ґрунтується на необхідності захисту інформації, яка циркулює всередині мережі.

Для розв'язання цих проблем використовують моніторинг та аналіз трафіку, які допомагають ефективно діагностувати та розв'язувати проблеми під час їх

виникнення, не даючи мережевому обладнанню простоювати довго. Оскільки інформація мережею передається майже безперервно, то стає зрозуміло, що припинення роботи обладнання або інші причини відмови в обслуговуванні призводять до збитків організацій або компаній, що надають послуги. У зв'язку з цим адміністраторам необхідно стежити за рухом мережевого трафіку і продуктивністю всієї мережі, а також перевіряти її на проломи в політиці безпеки.

3.7.1 Аналізатор трафіку WireShark

WireShark це відносно новий інструмент у сфері рішень для мережевої діагностики та аналізу, але незважаючи на те, що цей продукт ще молодий, це не завадило йому здобути собі визнання і повагу з боку IT-професіоналів.

WireShark чудово справляється з аналізом трафіку, прекрасно виконуючи для нас необхідну роботу. Адміністратори мереж змогли отримати чудовий продукт, що має середину між роботою з вихідними даними та візуальним представленням цих даних у наявному інтерфейсі, тому в WireShark ми не зможемо побачити перекосів у той чи інший бік, які можна побачити в більшій частині інших подібних рішень для аналізу та підготовки до аналізу мережевого трафіку. WireShark досить простий, сумісний з багатьма системами і портативний. Користувачі WireShark отримують саме той необхідний функціонал, що і хочуть, і отримують це швидко.

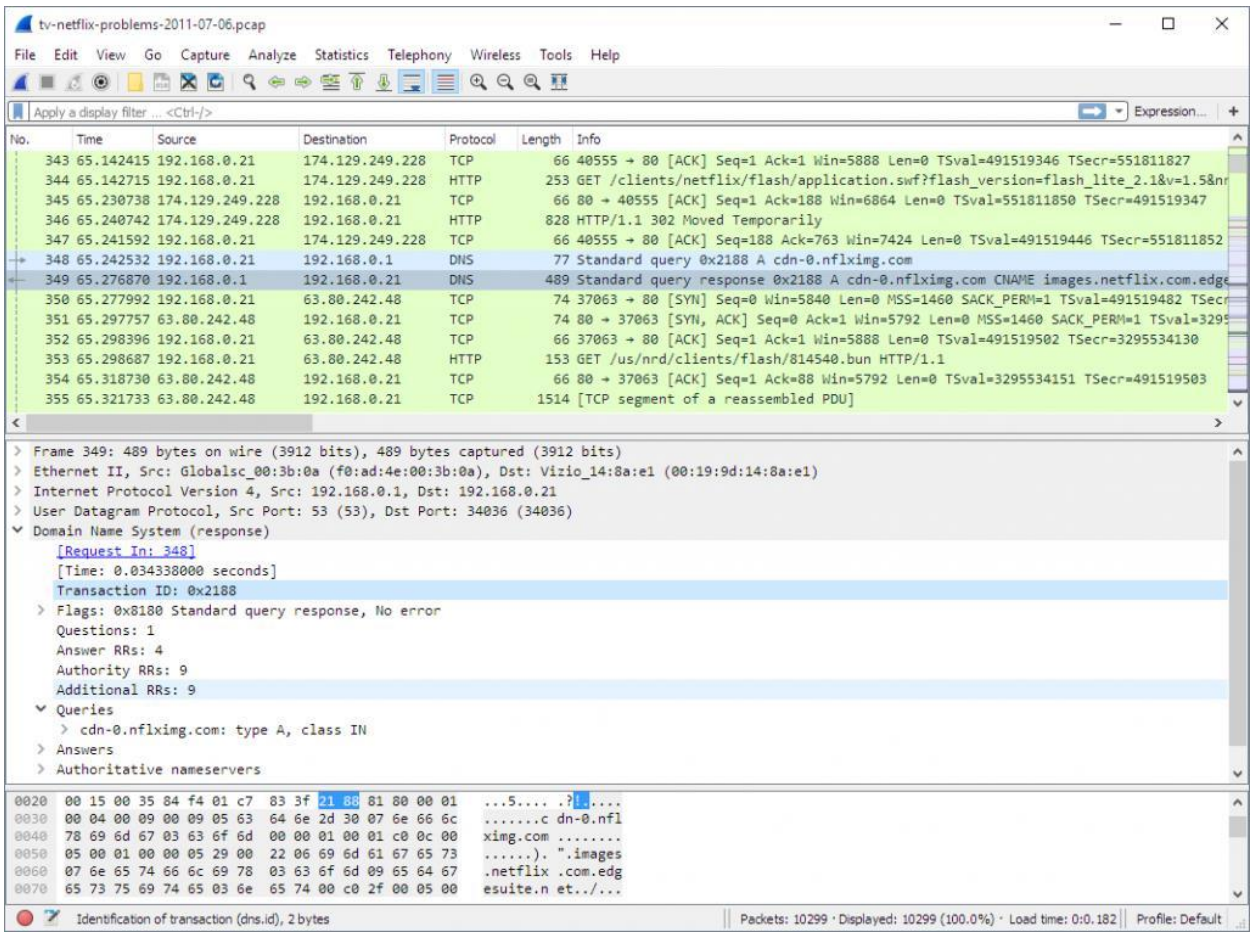


Рис. 3.2 Аналізатор трафіку Wireshark

WireShark володіє цілком зручним інтерфейсом користувача, досить великою кількістю опцій і функціоналом для фільтрації та сортування, але не для глибокого аналізу трафіку. Більшість користувачів цієї програми можуть оцінити дану програму, аналіз трафіку WireShark добре працює з усіма популярними операційними системами, наприклад: - *NIX, Windows і macOS.

Відмінність цієї технології від нашої в тому, що ми можемо проводити аналіз мережевих даних лише на одній конкретній ділянці мережі, а не на всьому маршруті даних.

3.7.2 Аналізатор трафіку tcpdump

Зовні аналізатор трафіку tcpdump вдає із себе якийсь інструмент, який використовували десятиліття тому, і, правду кажучи, якщо розглядати його з погляду функціональних можливостей, працює він так само, як досить старе

програмне забезпечення. Незважаючи на те, що з поставленими завданнями він справляється, водночас використовуючи для своїх можливостей мінімальну кількість ресурсів системи, зводячи до мінімуму навантаження на системи наскільки на скільки це взагалі можливо в умовах роботи програмного забезпечення.

Більшій частині сучасних користувачів буде дуже складно розібратися у великому розмаїтті таблиць з даними мережевого трафіку, що мають далеко не всю потрібну інформацію. Але все ж бувають ситуації, коли подібне програмне забезпечення може допомогти в розв'язанні будь-якої проблеми, використання полегшених і невимогливих до ресурсів рішень зможе бути корисним на практиці. У деяких середовищах або на досить слабкому за технічними характеристиками ПК мінімалізм може виявитися єдиним можливим до роботи варіантом.

Програмне забезпечення tcpdump було розроблено для середовища *NIX, але на поточний момент часу воно також добре працює з деякими іншими портами Windows. Воно має весь базовий функціонал, який ви можете побачити в будь-якому іншому аналізаторі трафіку - захоплення, запис тощо.

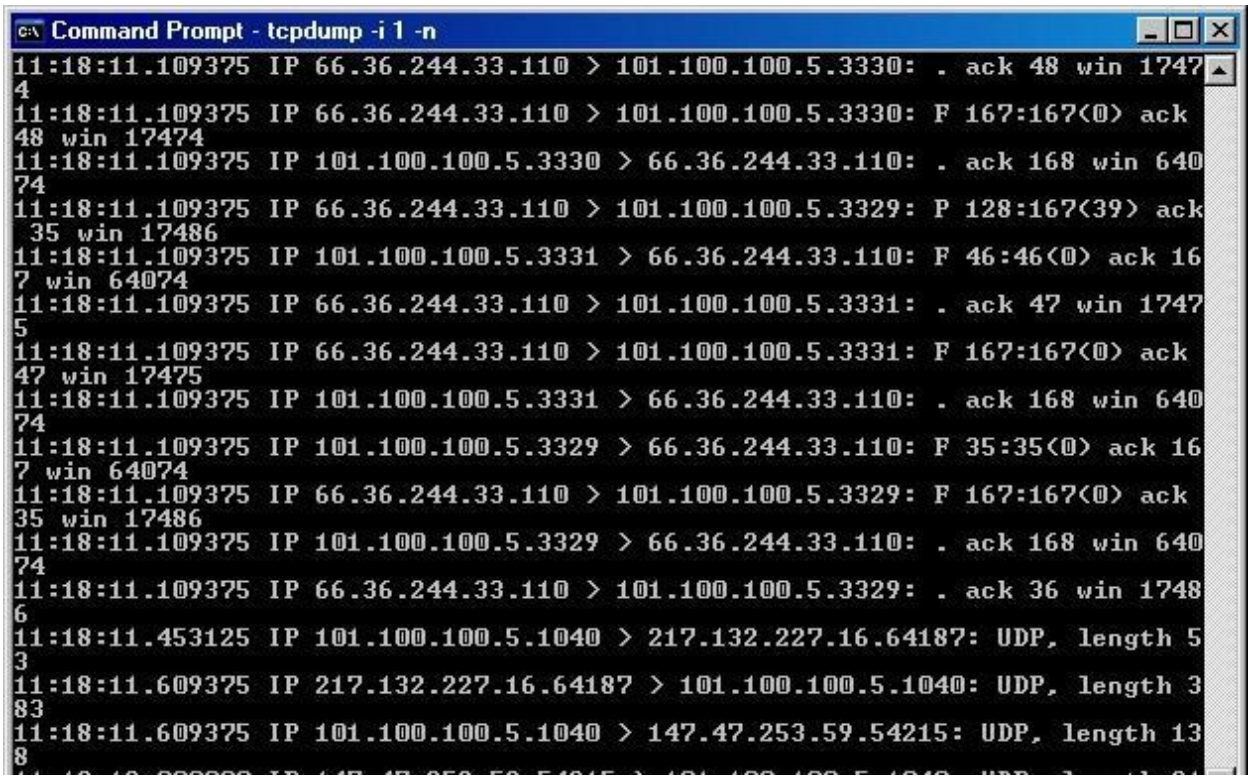


Рис. 3.3 Аналізатор трафіку tcpdump

У цьому випадку було виявлено недолік у тому, що програма має не зручний інтерфейс і відсутність захоплення пакетів у реальному часі.

3.7.3 Аналізатор трафіку Kismet

Kismet - це додатковий приклад програмного середовища з відкритим вихідним кодом, створеного для вирішення конкретних завдань, що виникають у нашій мережі. Kismet не обмежується на аналізі мережевого трафіку, він дає нам значно розширеніші функціональні можливості. Наприклад, це програмне забезпечення здатне здійснювати аналіз трафіку прихованих і бездротових мереж, які не транслюють свої ідентифікатори SSID. Цей інструмент буде дуже корисний, коли в нашій бездротовій мережі є щось, що може спричиняти проблеми, але швидко виявити їхнє джерело у нас не виходить. Kismet точно зможе допомогти нам виявити неавторизовану мережу або точку доступу, яка існує, але має неправильні налаштування.

Рис. 3.4 Аналізатор трафіку Kismet

3.7.4 Аналізатор трафіку EtherApe

Своїми функціональними здібностями EtherApe досить сильно схожий на WireShark, він так само є програмним середовищем з відкритим вихідним кодом і поширюється безкоштовно. Але, він дійсно дуже сильно відрізняється на тлі інших програмних забезпечень - головна відмінність полягає в тому, що він орієнтований на візуальне представлення даних за допомогою графічних можливостей інтерфейсу.

Якщо результати WireShark переглядаємо у звичному цифровому і табличному форматі, то весь трафік EtherApe демонструється з використанням просунутого графічного інтерфейсу, кожна вершина графа уособлює собою окремий пристрій, розміри цих самих вершин і ребер показують нам розмір мережевого трафіку на даному пристрої, а кольоровими маркерами відзначаються різні протоколи, які вдалося отримати. Користувачі, які віддають перевагу візуальному сприйняттю статистичної інформації, використовують аналізатор EtherApe. Доступний для середовищ UNIX і macOS.

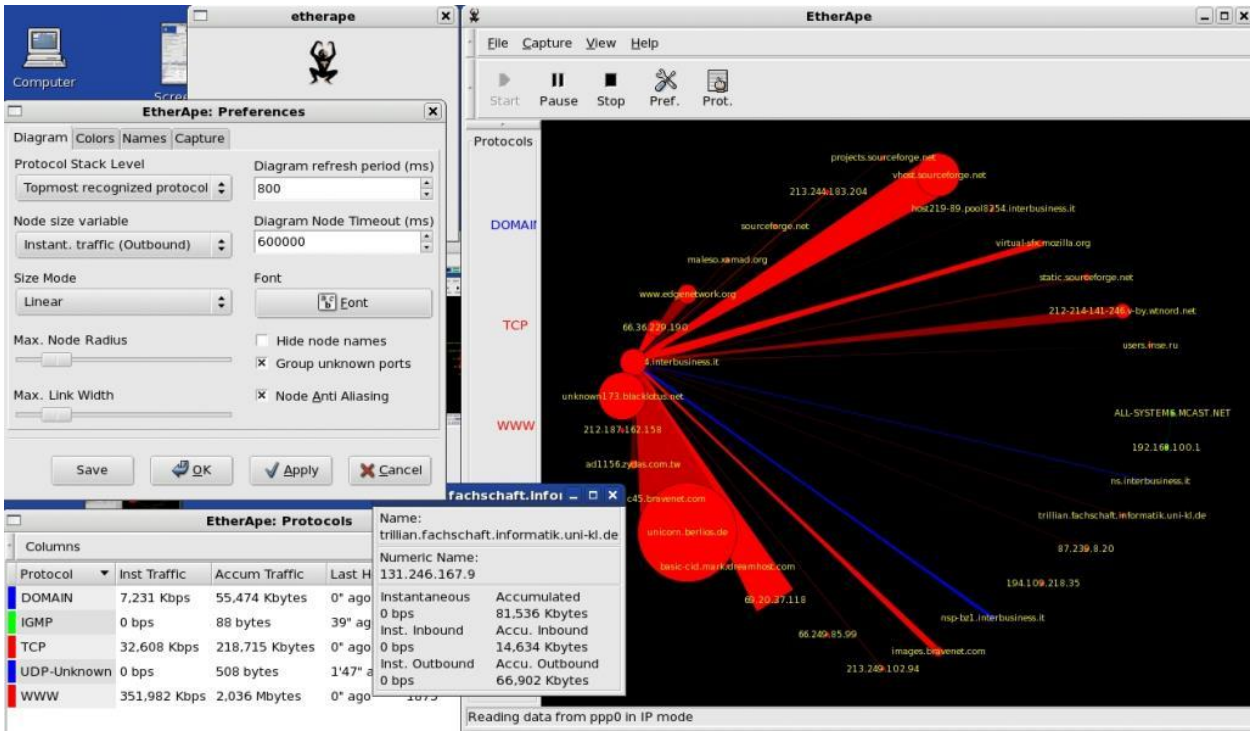


Рис. 3.5 Аналізатор трафіку EtherApe

3.7.5 Аналізатор трафіку Cain and Abel

У програмного середовища Cain and Abel, здатність аналізу трафіку є більше додатковою або допоміжною функцією, ніж основною. Коли завдання користувачів є не просто аналіз трафіку, то в більшості випадків згадують саме це програмне забезпечення. За допомогою цієї програми ми отримуємо можливість відновлювати загублені паролі для операційної системи Windows, здійснювати "атаки" для знаходження загублених облікових даних, одержувати дані VoIP у мережі, здійснювати аналіз і маршрутизацію пакетів, і деякі інші можливості.

Cain and Abel є потужним інструментом для досвідченого системного адміністратора з великою кількістю повноважень. Недоліком є те, що працювати він може тільки в середовищі Windows.

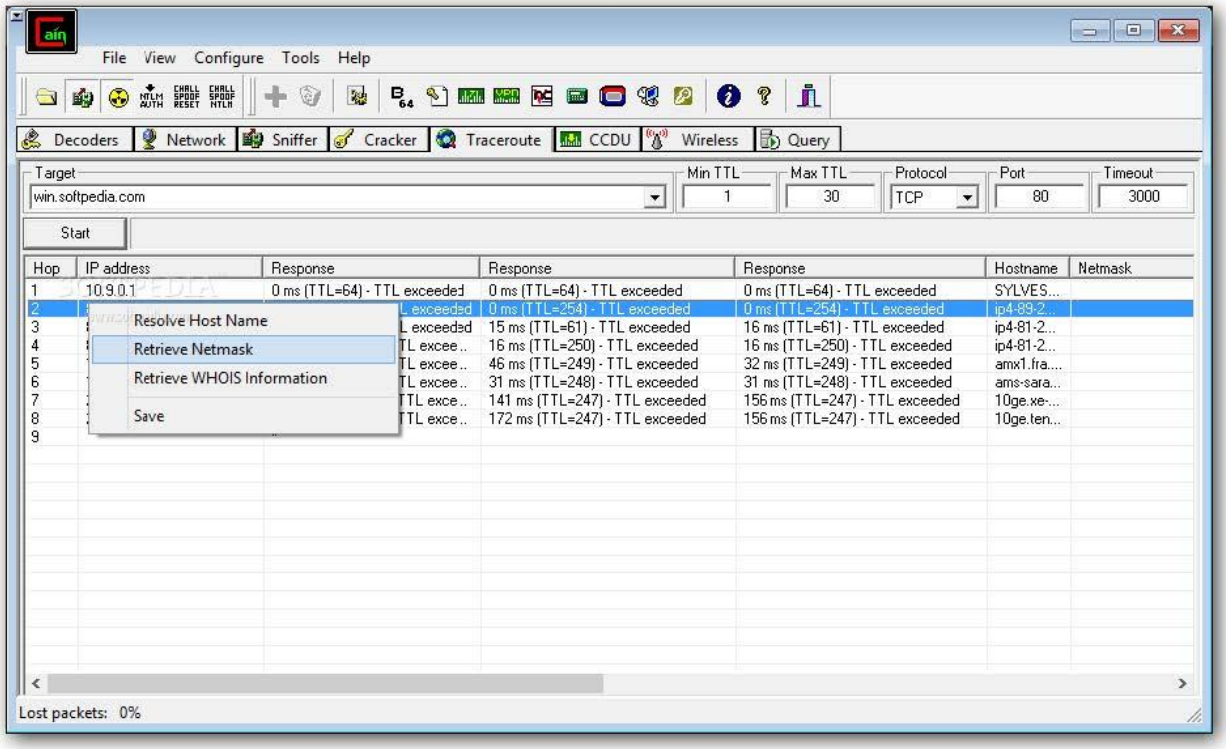


Рис. 3.6 Аналізатор трафіку Cain and Abel

Ця програма має функції відстеження даних користувачів і вразливостей мережі, але ми не можемо повністю контролювати всі ділянки мережі.

3.7.6 Аналізатор трафіку NetworkMiner

Програмне забезпечення NetworkMiner - ще одне рішення, чиї функціональні можливості перевершують рамки аналізатора трафіку. Більшість інших аналізаторів трафіку працюють на такі параметри як надсилання та отримання пакетів, NetworkMiner звертає увагу на те, хто і як здійснює ці надсилання та отримання. Це програмне забезпечення підходить для виявлення проблемних комп'ютерів або користувачів у нашій мережі, а не для глибокого аналізу даних, моніторингу або діагностики мережі як такої. Як і минуле програмне рішення NetworkMiner розроблено тільки для ОС Windows.

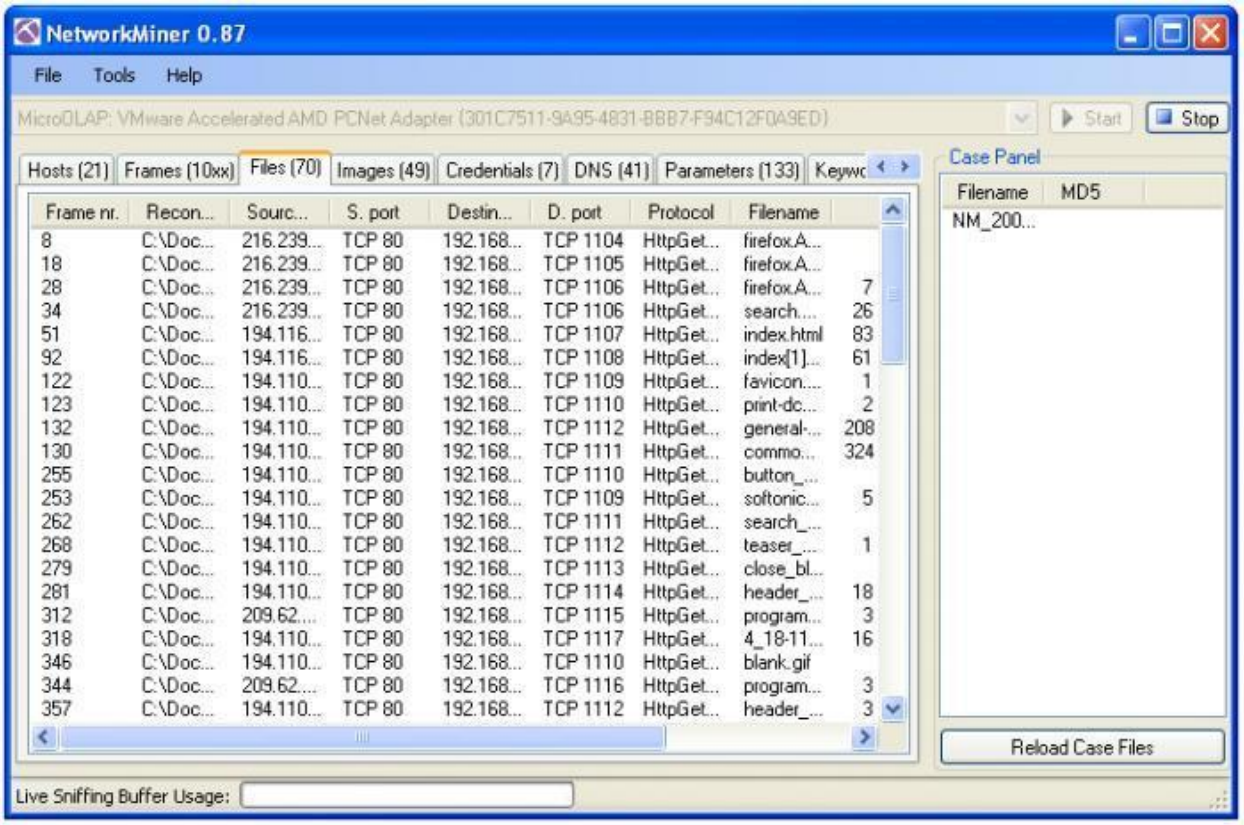


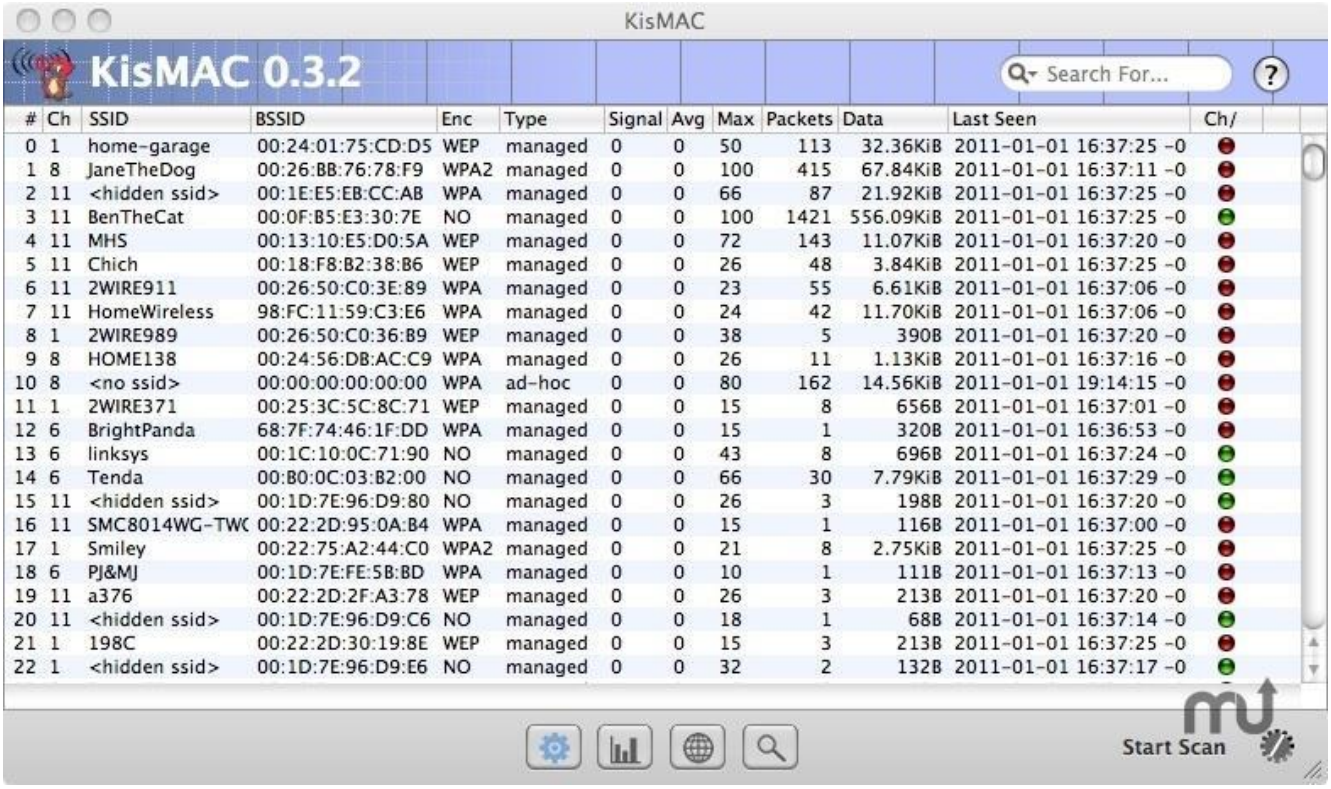
Рис. 3.7 Аналізатор трафіку NetworkMiner

Ця програма допомагає проаналізувати пропускну здатність мережі та пристроїв мережі, це не завжди допоможе нам виявити вразливості.

3.7.7 Аналізатор трафіку KisMAC

KisMAC - це описаний раніше Kismet, тільки більш зручно оформлений для macOS. Наразі Kismet має порт тільки для операційної системи macOS, через це ми можемо вважати, що існування KisMAC буде непотрібним, але нам необхідно звернути увагу на такий факт, як програмне забезпечення KisMAC має свою кодову базу і не належить до явних похідних аналізатора Kismet. Так само необхідно звернути увагу на те, що KisMAC дає нам деякі рідкісні можливості, як-от нанесення на мапу місця розташування пристроїв у мережі або атака деаутентифікації на операційній системі macOS.

Kismet не надає цей функціонал. Ці унікальні особливості в дуже рідкісних ситуаціях зможуть переважити вибір програмного забезпечення на користь саме цього рішення.



#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen	Ch/
0	1	home-garage	00:24:01:75:CD:D5	WEP	managed	0	0	50	113	32.36KiB	2011-01-01 16:37:25 -0	
1	8	JaneTheDog	00:26:BB:76:78:F9	WPA2	managed	0	0	100	415	67.84KiB	2011-01-01 16:37:11 -0	
2	11	<hidden ssid>	00:1E:E5:EB:CC:AB	WPA	managed	0	0	66	87	21.92KiB	2011-01-01 16:37:25 -0	
3	11	BenTheCat	00:0F:B5:E3:30:7E	NO	managed	0	0	100	1421	556.09KiB	2011-01-01 16:37:25 -0	
4	11	MHS	00:13:10:E5:D0:5A	WEP	managed	0	0	72	143	11.07KiB	2011-01-01 16:37:20 -0	
5	11	Chich	00:18:F8:B2:38:B6	WEP	managed	0	0	26	48	3.84KiB	2011-01-01 16:37:25 -0	
6	11	2WIRE911	00:26:50:C0:3E:89	WPA	managed	0	0	23	55	6.61KiB	2011-01-01 16:37:06 -0	
7	11	HomeWireless	98:FC:11:59:C3:E6	WPA	managed	0	0	24	42	11.70KiB	2011-01-01 16:37:06 -0	
8	1	2WIRE989	00:26:50:C0:36:B9	WEP	managed	0	0	38	5	390B	2011-01-01 16:37:20 -0	
9	8	HOME138	00:24:56:DB:AC:C9	WPA	managed	0	0	26	11	1.13KiB	2011-01-01 16:37:16 -0	
10	8	<no ssid>	00:00:00:00:00:00	WPA	ad-hoc	0	0	80	162	14.56KiB	2011-01-01 19:14:15 -0	
11	1	2WIRE371	00:25:3C:5C:8C:71	WEP	managed	0	0	15	8	656B	2011-01-01 16:37:01 -0	
12	6	BrightPanda	68:7F:74:46:1F:DD	WPA	managed	0	0	15	1	320B	2011-01-01 16:36:53 -0	
13	6	linksys	00:1C:10:0C:71:90	NO	managed	0	0	43	8	696B	2011-01-01 16:37:24 -0	
14	6	Tenda	00:B0:0C:03:B2:00	NO	managed	0	0	66	30	7.79KiB	2011-01-01 16:37:29 -0	
15	11	<hidden ssid>	00:1D:7E:96:D9:80	NO	managed	0	0	26	3	198B	2011-01-01 16:37:20 -0	
16	11	SMC8014WG-TWC	00:22:2D:95:0A:B4	WPA	managed	0	0	15	1	116B	2011-01-01 16:37:00 -0	
17	1	Smiley	00:22:75:A2:44:C0	WPA2	managed	0	0	21	8	2.75KiB	2011-01-01 16:37:25 -0	
18	6	PJ&MJ	00:1D:7E:FE:5B:BD	WPA	managed	0	0	10	1	111B	2011-01-01 16:37:13 -0	
19	11	a376	00:22:2D:2F:A3:78	WEP	managed	0	0	26	3	213B	2011-01-01 16:37:20 -0	
20	11	<hidden ssid>	00:1D:7E:96:D9:C6	NO	managed	0	0	18	1	68B	2011-01-01 16:37:14 -0	
21	1	198C	00:22:2D:30:19:8E	WEP	managed	0	0	15	3	213B	2011-01-01 16:37:25 -0	
22	1	<hidden ssid>	00:1D:7E:96:D9:E6	NO	managed	0	0	32	2	132B	2011-01-01 16:37:17 -0	

Рис. 3.8 Аналізатор трафіку KisMAC

Цю програму розроблено виключно під MAC ОС, у зв'язку з цим вона має дуже обмежену сферу застосування, і в нашому випадку ми не зможемо її використовувати на серверах з ОС Linux і Windows.

Останнім часом в галузі систем управління спостерігаються дві чітко виражені тенденції. По-перше, це інтеграція функцій управління мережами і системами в одному продукті. По-друге, це розподіленість систем управління, коли існує кілька консолей, які збирають інформацію про стан пристроїв і підсистем, а потім видають керівні дії. Це пояснюється тим, що більшість наявних систем є вузькоспеціалізованими і спрямованими на виконання конкретних функцій. Тому фахівцям доводиться використовувати зв'язку з декількома продуктами, щоб повністю охопити всі можливі вразливості мережі. Наприклад, системи моніторингу та обліку трафіку перевіряють працездатність обладнання та мережі, а системи виявлення та запобігання вторгненням допомагають виявити загрози всередині та ззовні мережі.

Сучасний підхід до побудови систем виявлення мережевих вторгнень та виявлення ознак комп'ютерних атак на інформаційні системи має свої недоліки і вразливості, які дозволяють зловмисним особам успішно обходити захист інформації.

На ринку представлено приблизно десяток систем запобігання та виявлення вторгнень, але всі вони мають важливий недолік: їхня робота заснована на правилах і шаблонах, тому не всі випадки вторгнень вдається виявити. Крім того, ці системи слабко справляються з "мімікруючим" шкідливим трафіком.

Варто також зазначити, що на ринку представлено небагато продуктів вітчизняних виробників у цій області. Крім того, раніше описані методики не завжди є доступними через їх комерційну таємницю. Тому виникає потреба у розробці нової системи, яка може застосовуватись в комплексі мережевих інструментів.

Тому, розроблена система буде програмою, яка складається з двох компонентів. Перша частина відповідає за захоплення даних з пристроїв на одному мережевому маршруті і зберігання їх у форматі pcap. Друга частина програми аналізує отримані дані з метою виявлення мережевих вразливостей, які можуть призвести до несанкціонованого доступу до розглянутої мережі.

ВИСНОВКИ ДО РОЗДІЛУ 3

В результаті виконання цього розділу дипломної роботи – була проаналізована та обґрунтована актуальність вивчення проблем забезпечення безпеки мережевого трафіку та мережі в цілому для захисту від несанкціонованого впливу, а також розглянуті існуючі підходи до вирішення цієї проблеми за допомогою використання сучасних методик аналізу мережевого трафіку. Було розглянуто кілька аналогів програм для роботи з даними мережі і після, встановлено, що жодна з цих програм не має функціоналу для аналізу трафіку на всіх ділянках мережі.

Тому, тепер ми маємо чітко сформульовані вимоги до розроблюваної системи.

ВИСНОВКИ

У ході виконання цієї дипломної роботи були проведені детальні дослідження щодо ролі Cloud-технологій у мультимедійних мережах й застосування технології Deep Packet Inspection (DPI) для захисту від DDoS-атак. Виявлено, що Cloud-технології є сучасним та перспективним підходом до розгортання та управління інформаційними системами, забезпечуючи гнучкість, ефективність та масштабованість.

Зокрема, застосування технології DPI для захисту від DDoS-атак є важливим етапом у забезпеченні безпеки хмарних сервісів та мереж. Використання DPI дозволяє аналізувати та фільтрувати мережевий трафік, ідентифікувати та блокувати шкідливі пакети, що дозволяє знизити вплив DDoS-атак на інфраструктуру та забезпечити нормальну роботу мережі та сервісів.

Загалом, результати цієї дипломної роботи підтверджують важливість Cloud-технологій та застосування технології DPI для забезпечення безпеки мереж та інформаційних систем. Cloud-технології дозволяють покращити доступність, ефективність та масштабованість інфраструктури, забезпечуючи гнучкість та зниження витрат. Водночас, застосування DPI стає необхідним для виявлення та мінімізації впливу DDoS-атак на системи, дозволяючи аналізувати та фільтрувати мережевий трафік.

Проте, важливо враховувати обмеження технології DPI, такі як великі обчислювальні витрати та можливість помилок аналізу пакетів. Це вимагає ретельної настройки та постійного підтримання системи DPI з урахуванням особливостей мережі та типів атак.

Майбутні дослідження можуть спрямовуватися на подальше вдосконалення технологій Cloud та DPI. Розробка нових методів аналізу та фільтрації трафіку, оптимізація ресурсних витрат технології DPI та розширення її можливостей є актуальними завданнями. Також важливо проводити дослідження в області розробки

адаптивних систем, які здатні швидко реагувати на нові види DDoS-атак та адаптуватися до змін у мережі.

Загальною метою цих напрямків досліджень є забезпечення безпеки, доступності та надійності мереж та інформаційних систем, що стає все важливішим у сучасному цифровому світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. О. Г. Пасічник, О. В. Пасічник, І. В. Стеценко «Основи веб-дизайну»
2. «Computer Speech Technology», Роберт Родман [2009]
3. "DPI for Dummies" - Автор: Joel Snyder (2021).
4. Мартиненко В. І. Захист мереж інформаційного зв'язку в умовах кібербезпеки: монографія. – К.: Аграр Медіа Груп, 2020.
5. "DDoS Attacks and Defense Mechanisms: Practical Insights and Solutions" - Автор: Shon Harris, Michael Lester, Joshua New (2021).
6. "Security Operation Center (SOC) for Dummies" - Автор: Amy E. McDougall, Brian Kelley (2021).
7. Балабанов О. Г., Лук'янова Н. В., Пархоменко А. А. Інформаційна безпека: теорія та практика: монографія. – К.: ВПЦ «Київський університет», 2020.
8. "Machine Learning for DDoS Detection and Mitigation: Techniques and Applications" - Автор: Yang Xiang, Xianghui Cao, Wanlei Zhou (2021).
9. "Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare" - Автор: Thomas A. Johnson (2021).
10. Самойленко А. А., Єрмолаєв О. І. Комп'ютерна безпека: підручник для студентів вищих навчальних закладів. – К.: НТУУ «КПІ», 2021.
11. "Practical Internet of Things Security: Designing and Building Secure IoT Networks and Cloud Architectures" - Автор: Brian Russell, Drew Van Duren, John Matlock (2021).
12. "Network Security: Private Communication in a Public World" - Автор: Charlie Kaufman, Radia Perlman, Mike Speciner (2021).
13. Львівський С. В., Білоус О. О., Виноградов О. В. Захист комп'ютерних мереж: підручник. – К.: КНЕУ, 2020.
14. Косенко В. О., Курганський В. С. Кібербезпека: основні аспекти захисту від кіберзлочинів та кібертероризму. – К.: ВПЦ «Київський університет», 2020.

15."Securing the Cloud: Cloud Computer Security Techniques and Tactics" - Автори: Vic (J.R.) Winkler, Prashant Haldankar (2022).