ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технологія аналізу мережевого трафіку для виявлення аномалій в інформаційній системі на базі Cisco Stealthwatch»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Воскобойник О.В.
(прізвище та ініціали)
Керівник Дмітрієв В.Є.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Воскобойнику Олексію Володимировичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія аналізу мережевого трафіку для виявлення аномалій в інформаційній системі на базі Cisco Stealthwatch»

керівник магістерської роботи Дмітрієв Вячеслав Євгенійович, ст.викладач
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «13» жовтня 2020 року № 230.

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи
інформаційна система;
програмний комплекс для захисту кінцевих точок;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту кінцевих точок інформаційних систем.
2. Аналіз сучасних загроз кінцевих точок.
3. Методи та засоби управління захистом кінцевих точок.
4. Варіант технології захисту кінцевих точок інформаційної системи.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу проблеми забезпечення безпеки кінцевих точок в інформаційних системах.

4. Результати аналізу методів та засобів захисту кінцевих точок.

5. Призначення, можливості та функції Cisco AMP for Endpoint.

6. Архітектура та компоненти Cisco AMP for Endpoint.

7. Додатки платформи Cisco AMP for Endpoint.

8. Варіант технології захисту кінцевих точок інформаційної системи.

9. Висновки за результатами роботи.

6. Дата видачі завдання 01.10.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок інформаційних систем.	09.10.2021 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	29.10.2021 р.	
3.	Аналіз методів та засобів захисту кінцевих точок.	15.11.2021 р.	
4.	Розроблення варіанту технології захисту кінцевих точок інформаційної системи.	24.11.2021 р.	
5.	Розроблення рекомендацій щодо застосування технології захисту кінцевих точок інформаційної системи.	03.12.2021 р.	
6.	Оформлення результатів дослідження.	10.12.2021 р.	
7.	Підготовка доповіді до захисту.	15.12.2021 р.	

Студент Воскобойник О.В.
(підпис) прізвище та ініціали

Керівник магістерської роботи Дмітрієв В.Є.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Воскобойника Олексія Володимировича
на тему: «Технологія аналізу мережевого трафіку для виявлення аномалій в інформаційній системі на базі Cisco Stealthwatch»

Актуальність:
Одним із проявів процесу інформатизації суспільства є масштабний розвиток мережевих сервісів. Перед адміністраторами інформаційно-обчислювальних систем, що надають послуги, стоїть завдання забезпечити керованість та підзвітність цих систем, цілісність, доступність та конфіденційність даних, тобто забезпечити штатне функціонування системи та максимально виключити факти нештатного функціонування – мережеві аномалії.

Позитивні сторони:
1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми забезпечення захисту комп'ютерних мереж інформаційної системи від аномалій трафіку, визначена мета та завдання технології захисту комп'ютерних мереж інформаційної системи.
2. Було досліджено методи та засоби захисту комп'ютерних мереж інформаційної системи на базі Cisco Stealthwatch.
3. Запропоновано варіант технології захисту комп'ютерних мереж на базі рішення Cisco Cisco Stealthwatch та рекомендації щодо її застосування.

Недоліки:
1. У магістерській роботі слідувало б провести більш детальний опис принципів роботи системи на базі Cisco Stealthwatch.
2. Запропонований варіант технології захисту кінцевих точок інформаційної системи на базі Cisco Stealthwatch бажано було б показати на прикладі конкретного підприємства.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку **задовільно**, а студент **Воскобойник О.В.** – присвоєння кваліфікації 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Воскобойник О.В. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія аналізу мережевого трафіку для виявлення аномалій в інформаційній системі на базі Cisco Stealthwatch».

Магістерська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Воскобойник О.В. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Журенко О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Воскобойник О.В.*** обрав тему роботи, метою якої було дослідити зміст технології захисту комп'ютерних мереж на базі Cisco Stealthwatch. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Воскобойник О.В. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Воскобойника О.В. на оцінку **«задовільно»** та присвоїти йому кваліфікацію 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

Керівник магістерської роботи _____ Дмітрієв В.Є.
(підпис) (прізвище та ініціали)
"____" _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Воскобойник О.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

"____" _____ 2021 року

РЕФЕРАТ

Текстова частина магістерської роботи: 65 сторінок, 11 рисунків, 2 таблиці, 15 джерел.

Об'єкт дослідження – процес забезпечення захисту комп'ютерних мереж інформаційної системи.

Предмет дослідження – технологія захисту комп'ютерних мереж інформаційної системи.

Мета роботи – розробити варіант системи захисту комп'ютерних мереж інформаційної системи та рекомендації щодо застосування технології їх захисту на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту кінцевих точок інформаційної системи.

В роботі зроблено аналіз проблеми забезпечення кібербезпеки інформаційної системи, визначено основні типи атак комп'ютерні мережі та визначено мету та завдання захисту кінцевих точок інформаційної системи. Проведено аналіз та порівняння існуючих технологій захисту комп'ютерних мереж інформаційної системи.

Досліджено методи та засоби захисту кінцевих точок на прикладі Cisco Stealthwatch. Визначено призначення, основні функції та склад рішення Cisco Stealthwatch.

На основі досліджень проведених в роботі розроблено варіант технології захисту комп'ютерних мереж інформаційної системи та рекомендації щодо застосування даної технології на підприємстві.

Галузь використання – кібербезпека інформаційної системи.

ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ЗАХИСТ КОМП'ЮТЕРНИХ МЕРЕЖ, АНАЛІЗ МЕТОДІВ, ТЕХНОЛОГІЇ ВИЯВЛЕННЯ, ВРАЗЛИВІСТЬ, ЗАГРОЗА, БЕЗПЕКА, АНОМАЛІЇ, МЕРЕЖЕВИЙ ТРАФІК.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

LAN – Local Area Network

WAN – Wide Area Network

P2P – Peer to Peer

КС – комп’ютерна система

ОС – операційна система

ПЗ – програмне ззабезпечення

SQL – structured query language

DDoS – Distributed-denial-of-service

VLAN – Virtual Local Area Network

NAT – Network Address Translation

DNS – Domain Name System

SNMP – Simple Network Management Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol,

ICMP – Internet Control Message Protocol

ВСТУП

Актуальність дослідження. Мережеві аномалії мають різні причини і можуть бути пов'язані з діяльністю хакерів, некомпетентних користувачів, несправністю апаратури та дефектами програмного забезпечення. Існують видимі аномалії, що виявляються у некоректній роботі інформаційно-обчислювальної системи. Аномалії можуть і не мати видимих ознак, але призвести до збоїв через тривалий час.

Виявлення мережевих аномалій можливе за допомогою використання систем моніторингу – комплексу заходів, спрямованих на отримання відомостей про стан системи для прийняття рішень щодо реакції на події. Ефективність системи моніторингу безпосередньо залежить від компонентів, що входять до її складу, кожен з яких виконує свою функцію. При цьому при проектуванні подібних систем необхідно враховувати цільову аудиторію, параметри підсистеми, що відстежується, умови переходів від одного стану в інший, частоту оновлення і спосіб зберігання даних. Окремо можна виділити формат представлення даних користувачеві.

Для забезпечення ефективного захисту комп’ютерних мереж використовуються нові підходи й рішення, що забезпечують комплексний захист.

Фахівцям із кібербезпеки, які відповідальні за захист комп’ютерних мереж, необхідно приділяти особливу увагу виявленню аномалій трафіку, так-як є потребність постійного моніторингу та аналізу вибраних мережевих показників.

Об’єкт дослідження – процес забезпечення захисту комп’ютерних мереж інформаційної системи.

Предмет дослідження – технологія захисту комп’ютерних мереж інформаційної системи.

Мета роботи – розробити варіант системи захисту комп’ютерних мереж інформаційної системи та рекомендації щодо застосування технології їх захисту на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту кінцевих точок інформаційної системи.

Практичне значення одержаних результатів полягає в розробці варіанта технології забезпечення безпеки комп’ютерних мереж інформаційної системи на базі рішення Cisco Stealthwatch та рекомендації щодо її застосування на підприємстві.

1 АНАЛІЗ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

1.1. Основні характеристики комп'ютерних мереж в інформаційній системі

Комп'ютерна мережа – це система, яка з'єднує численні незалежні комп'ютери з метою обміну інформацією (даними) та ресурсами. Інтеграція комп'ютерів та інших різних пристроїв дозволяє користувачам спілкуватися легше.

Комп'ютерна мережа – це сукупність двох або більше комп'ютерних систем, пов'язаних між собою. Підключення до мережі можна встановити за допомогою кабельного або бездротового медіа. Апаратне та програмне забезпечення використовуються для підключення комп'ютерів та інструментів у будь-яку мережу.

Комп'ютерна мережа складається з різноманітних вузлів. Сервери, мережеве обладнання, персональні комп'ютери та інші вузли спеціалізованого або загального призначення можуть бути вузлами комп'ютерної мережі. Для їх ідентифікації використовуються імена хостів та мережеві адреси.

Мета створення мережі:

- Програми не повинні виконуватися в одній системі через розподіл ресурсів і навантаження.
- Зменшення витрат – кілька машин можуть спільно використовувати принтери, стрічкові накопичувачі та інші периферійні пристрої.
- Надійність – якщо одна машина виходить з ладу, на її місце може прийти інша.
- Масштабованість (просто додати більше процесорів або комп'ютерів)
- Зв'язок і пошта (люди, які живуть окремо, можуть працювати разом)

- Доступ до інформації (віддалений доступ до інформації, доступ до Інтернету, електронної пошти, відеоконференції та інтернет-магазини).
- Інтерактивні розваги (ігри в Інтернеті, відео тощо).
- Соціальні мережі.

Типи мереж:

1. *Поділ на основі засобу зв'язку*

Дротова мережа: як ми всі знаємо, «дротова» означає будь-який фізичний носій, що складається з кабелів. Мідний дріт, вита пара або волоконно-оптичні кабелі – усі варіанти. У дротовій мережі використовуються дроти для підключення пристроїв до Інтернету чи іншої мережі, наприклад, ноутбуків або настільних ПК.

Бездротова мережа: «Бездротова» означає бездротовий носій, який складається з електромагнітних хвиль (EM Waves) або інфрачервоних хвиль. Антени або датчики будуть присутні на всіх бездротових пристроях. Прикладами бездротових пристроїв є мобільні телефони, бездротові датчики, пульти дистанційного керування телевізором, приймачі супутникових дисків і ноутбуки з картами WLAN. Для передачі даних або голосового зв’язку бездротова мережа використовує радіочастотні хвилі, а не дроти.

2. *Поділ на основі охопленої території*

Локальна мережа (LAN): LAN — це мережа, яка охоплює територію близько 10 кілометрів. Наприклад, мережа коледжів або офісна мережа.

Мережа столичного району (MAN): MAN відноситься до мережі, яка охоплює все місто. Наприклад: мережа кабельного телебачення.

Глобальна мережа (WAN): WAN відноситься до мережі, яка з'єднує країни або континенти. Наприклад, Інтернет дозволяє користувачам отримати доступ до розподіленої системи під назвою www з будь-якої точки земної кулі.

3. *На основі видів спілкування*

Мережі «точка-точка»: мережа «точка-точка» — це тип мережі передачі даних, що встановлює прямий зв'язок між двома вузлами мережі.

Прямий зв’язок між двома пристроями, такими як комп’ютер і принтер, відомий як з’єднання «точка-точка».

Трансляційні мережі: у мережах мовлення — метод сигналу, за якого численні сторони можуть почути одного відправника. Радіостанції є чудовою ілюстрацією «Мережі мовлення» у повсякденному житті. У цьому сценарії радіостанція є відправником даних/сигналу, і дані призначені для переміщення лише в одному напрямку. Подалі від вежі радіопередавання, якщо бути точним.

4. Залежно від типу архітектури

Мережі P2P: комп’ютери з подібними можливостями та конфігураціями називаються одноранговими.

«P2P» — це абревіатура від «peer to peer». «Рівні» в одноранговій мережі – це комп’ютерні системи, з’єднані одна з одною через Інтернет. Без використання центрального сервера файли можна обмінювати безпосередньо між системами в мережі.

Мережі клієнт-сервер: кожен комп’ютер або процес у мережі є або клієнтом, або сервером в архітектурі клієнт-сервер. Клієнт запитує послуги у сервера, які надає сервер. Сервери – це високопродуктивні комп’ютери або процеси, які керують дисководами (файловими серверами), принтерами (серверами друку) або мережевим трафіком (мережевими серверами)

Гібридні мережі: гібридна модель відноситься до мережі, яка використовує комбінацію архітектури клієнт-сервер і однорангової архітектури. Наприклад: Торрент.

Топологія мережі

1) Топологія із загальною шиною (англ. Bus Topology)

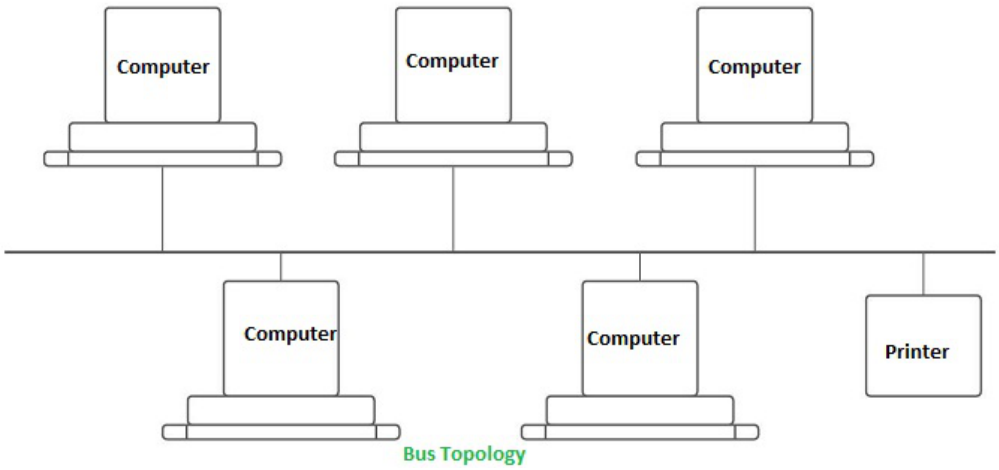

Рис. 1.1. Приклад топології з загальною шиною

Одна із перших фізичних топологій. Суть полягала в тому, що до одного довгого кабелю приєднували всі пристрої та організовували локальну мережу. На кінцях кабелю були потрібні термінатори. Як правило, це був опір на 50 Ом, який використовувався для того, щоб сигнал не відображався в кабелі. Перевага її була лише у простоті установки. З погляду працездатності була вкрай стійкою. Якщо десь у кабелі відбувався розрив, вся мережа залишалася паралізованою, до заміни кабелю.

2) Кільцева топологія (англ. Ring Topology)

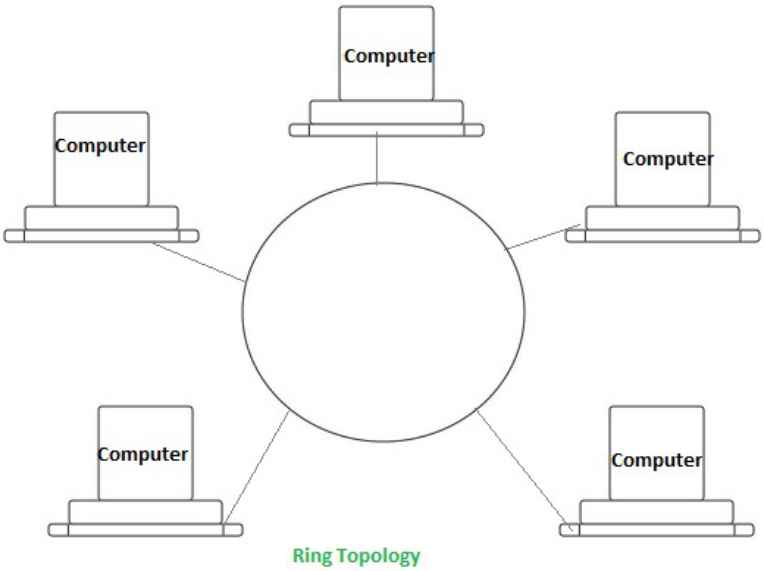

Рис. 1.2. Приклад кільцевої топології

У цій топології кожен пристрій підключається до двох сусідніх. Створюючи таким чином кільце. Тут логіка така, що з одного кінця комп'ютер тільки сприймає, а з іншого тільки відправляє. Тобто виходить передача по кільцю і наступний комп'ютер грає роль ретранслятора сигналу. За рахунок цього потреба у термінаторах відпала. Відповідно, якщо десь кабель ушкоджувався, кільце розмикалося і мережа ставала непрацездатною. Для підвищення стійкості до відмов, застосовують подвійне кільце, тобто в кожен пристрій приходить два кабелі, а не один. Відповідно, при відмові одного кабелю залишається працювати резервний.

3) Топологія зірка (англ. Star Topology)

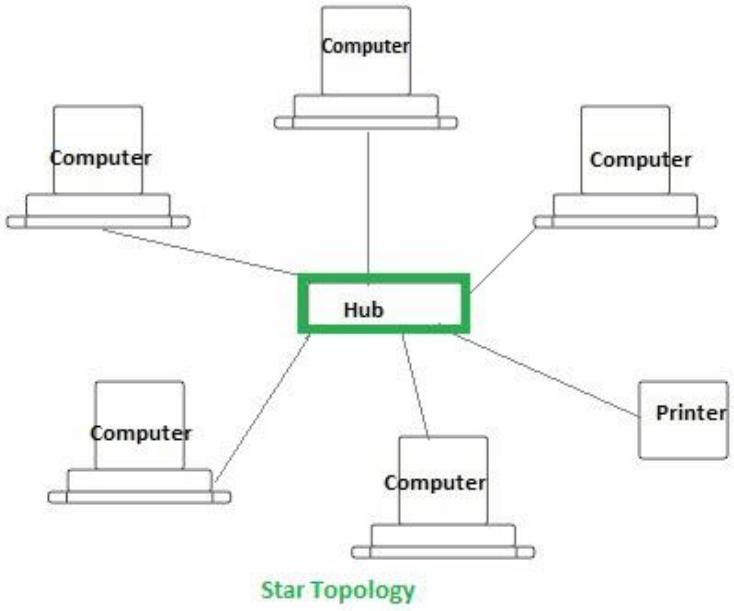

Рис. 1.3. Приклад топології зірка

Усі пристрої підключаються до центрального вузла, який є ретранслятором. В даний час ця модель використовується в локальних мережах, коли до одного комутатора підключаються кілька пристроїв, і він є посередником у передачі. Тут відмовостійкість значно вища, ніж у попередніх двох. При обриві якого-небудь кабелю випадає з мережі тільки один пристрій. Решта продовжують спокійно працювати. Однак, якщо відмовить центральну ланку, мережа стане непрацездатною.

4) Повнозв'язна топологія (англ. Full-Mesh Topology)

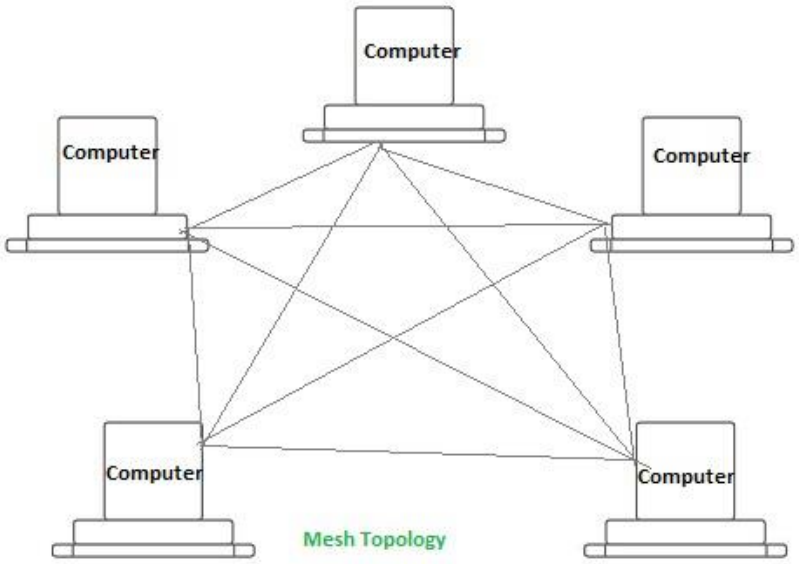

Рис. 1.4. Приклад повнозв’язної топології

Всі пристрої пов'язані безпосередньо один з одним. Тобто, з кожного на кожен. Ця модель є, мабуть, найвідмовнішою, тому що не залежить від інших. Але будувати мережі на такій моделі складно та дорого. Оскільки в мережі, що має мінімум 1000 комп'ютерів, доведеться підключати 1000 кабелів на кожен комп'ютер.

5. Топологія дерева (з англ. Tree Topology)

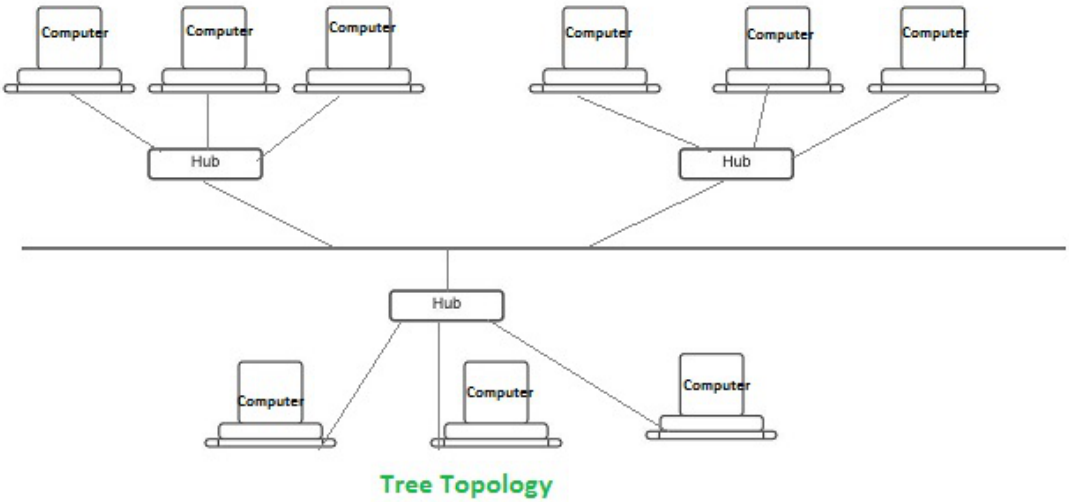

Рис. 1.5. Приклад топології дерева

Топологія дерева схожа на топологію зірки. Вузли в дереві, як і в зірці, підключені до центрального концентратора, який керує мережевим трафіком. Він має кореневий вузол, який з’єднаний з усіма іншими вузлами, створюючи ієрархію. Ієрархічна топологія - це інша назва. Кількість мереж Star підключено через шину в топології дерева.

Інформаційна безпека комп'ютерної мережі (КС) - це її властивість протистояти спробам завдати шкоди власникам і користувачам мережі під час різних навмисних і ненавмисних впливів на неї. Іншими словами, це захист мережі від випадкового або навмисного втручання в нормальний процес її функціонування, а також від спроб крадіжки, модифікації або знищення інформації, що циркулює в мережі.

Визначено три основні принципи інформаційної безпеки, які мають забезпечити:

• конфіденційність інформації, тобто її властивість бути відомою лише допущеним (авторизованим) суб'єктам мережі (користувачам, програмам, процесам);

• цілісність даних (ресурсу) мережі, тобто властивість даних бути в семантичному сенсі незмінними під час роботи мережі, що досягається за рахунок захисту даних від збоїв і несанкціонованого доступу до них;

• доступність інформації в будь-який час для всіх авторизованих користувачів.

Розрізняють зовнішню та внутрішню охорону компресорної станції. Предметом зовнішньої безпеки є забезпечення захисту КС від зловмисників ззовні з метою крадіжки, доступу до носіїв даних, виведення з ладу мережі, а також захисту від стихійних лих. Внутрішня безпека включає забезпечення надійної роботи мережі, цілісності її програм і даних.

У рамках комплексного розгляду питань забезпечення інформаційної безпеки КС розрізняє загрози безпеці, служби безпеки та механізми реалізації функцій служб безпеки.

Класифікація загроз інформаційній безпеці КС. Нижче наведена класифікація навмисних загроз безпеці КС, а також виділені лише основні види загроз. Під

загрозою безпеці розуміють потенційний вплив на КС, що прямо чи опосередковано завдає збитків власникам або користувачам мережі.

Реалізація загрози називається нападом.

Загрози можна класифікувати за такими критеріями :

1. За метою впровадження:

• порушення цілісності інформації, що може призвести до втрати або знецінення інформації;

• порушення конфіденційності інформації (використання цінної інформації іншими особами завдає істотної шкоди інтересам її власників);

• часткове або повне порушення роботи (доступності) КС.

2. За принципом впливу на мережу:

• використання доступу суб'єкта КС (користувача, процесу) до об'єкта (файлу даних, каналу зв'язку). Доступ — це взаємодія між суб'єктом і об'єктом (перший виконує певну операцію над другим), що призводить до виникнення інформаційного потоку від другого до першого;

• використання прихованих каналів, тобто шляхів передачі інформації, що дозволяють взаємодіючим процесам (суб'єктам) обмінюватися інформацією у спосіб, що порушує політику безпеки системи.

3. За характером впливу на мережу:

• активний вплив, пов'язаний із здійсненням зловмисником будь-яких дій: доступ до певних наборів даних, програм, злом паролів тощо. Такий вплив може здійснюватися як за допомогою доступу, так і за допомогою доступу, та за допомогою прихованих каналів. Це призводить до зміни стану мережі;

• пасивний вплив, що здійснюється шляхом спостереження будь-яких побічних ефектів (наприклад, від роботи програми) та їх аналізу. Пасивне розкриття завжди пов'язане лише з порушенням конфіденційності інформації в КС, оскільки під час нього не вживаються дії з суб'єктами та об'єктами. Це не змінює стан системи.

У свою чергу, активним навмисним впливом може бути:

• короткострокові, що вказують на випадковість або небажання зловмисника привернути увагу (воно менш небезпечне, але має більше шансів залишитися непоміченим), або довгострокове, пов'язане зі стійким інтересом до чужого інформаційного простору з метою вивчення його структура та зміст;

• неруйнівний, коли мережа продовжує нормально функціонувати, оскільки в результаті такого впливу ні програми, ні дані не були пошкоджені, але можлива крадіжка інформації та порушення її конфіденційності.

Якщо це не випадково, то це дуже небезпечно і свідчить про намір зловмисника використати знайдений канал доступу до чужої інформації в майбутньому;

• деструктивні, коли в результаті впливу на інформаційне середовище вносяться будь-які зміни в програми та/або дані, що впливає на роботу мережі. При належному архівуванні його наслідки можна усунути відносно легко;

• одноразовий або багаторазовий, що свідчить про серйозність намірів зловмисника і вимагає рішучої реакції;

• зареєстрованим адміністратором мережі при проведенні періодичного аналізу реєстраційних даних вказує на необхідність покращення або модифікації системи захисту;

• незареєстрований адміністратор мережі.

4. За методом активного впливу на об'єкт нападу:

• прямий вплив, наприклад, прямий доступ до файлів даних, програм, каналу зв'язку тощо. Таку дію зазвичай легко запобігти за допомогою контролю доступу;

• Вплив на систему дозволів (включаючи захоплення привілеїв). Тут здійснюються несанкціоновані дії щодо прав на об'єкт атаки, а доступ до самого об'єкта потім здійснюється у законний спосіб;

• непрямий вплив (через інших користувачів), наприклад, коли зловмисник якимось чином привласнює собі повноваження авторизованого користувача, видаючи себе за нього, або через використання вірусу, коли вірус виконує необхідні дії та повідомляє про результат особа, яка ввела його. Цей метод особливо небезпечний.

Необхідний постійний контроль як з боку адміністраторів і операторів за роботою мережі в цілому, так і з боку користувачів за своїми наборами даних.

5. За допомогою засобів атаки використовуються:

• використання зловмисником стандартного програмного забезпечення. У цьому випадку результати втручання зазвичай передбачувані, оскільки більшість стандартних програм добре вивчені;

• використання спеціально розроблених програм, що пов'язано з великими труднощами, але може бути більш небезпечним для мережі.

6. За станом об'єкта нападу:

• вплив на об'єкт атаки, коли на момент атаки він знаходиться в стані зберігання інформації (на диску, магнітній стрічці, в оперативній пам'яті). У цьому випадку вплив на об'єкт зазвичай здійснюється з використанням несанкціонованого доступу;

• вплив на об'єкт при передачі інформації по лінії зв'язку між вузлами мережі або всередині вузла. У цьому штаті предмет, вплив на нього передбачає ефірний доступ до фрагментів переданої інформації або прослуховування за допомогою прихованих каналів;

• вплив на об'єкт, коли він знаходиться в стані обробки інформації. Тут, націлення на атаку є процесом користувача.

Наведені категорії можуть бути складністю визначення їх загроз та шляхів їх реалізації. Звідси висновок: універсального методу захисту, який би запобігти будь-якій загрозі, не існує. Це необхідна для з'єднання різних аспектів безпеки, щоб забезпечити інформаційний захист від вашої мережі як цілісності.

У додатку до списку загроз до інформації безпеки слід додати такі загрози:

• несанкціонований обмін інформацією між користувачами, які можуть бути отримані в одному з них інформацією, що не вводиться для нього;

• відмова від інформації, тобто невизнання одержувачем (відправником) цієї інформації факту її отримання (надсилання), які можуть вестися до різних зловживань;

• посилання на службу, яка може мати певні наслідки для користувача, що потребує оцінки послуг мережі.

У випадку розв'язання проникнення в мережу, наступні типи розрізняють вплив на інформацію:

• знищення, тобто фізичне видалення інформації з носіїв інформації (виявляється при першій спробі доступу до цієї інформації, і всі втрати легко відновлюються за допомогою встановленої системи резервного копіювання та архівування);

• спотворення - порушення логіки роботи програм або зв'язків у структурованих даних, що не викликає відмови в їх роботі або використанні (тому це один з найменших типів впливу, оскільки його неможливо виявити);

• знищення - здатність до програми цілісності і структури даних, викликаючи неможливість їх використання: програми, що не запускаються, і коли доступ до структурованих, часто виникає помилка;

• заміна - заміна існуючих програм або даних іншими з такою ж назвою і таким чином, щоб вони не виглядали зовні. Це також небезпечний тип впливу; Надійним способом захисту від нього є порозрядне порівняння з еталонною версією програми;

• копіювання, тобто отримання копії програм або даних на іншому комп'ютері. Цей вплив є найбільш згубним в умовах промислового шпигунства, але це не є вірогідним нормальним функціонуванням мережі;

• Призначення нових компонентів, що є, записуючи інші дані або програми в комп'ютері пам'яті, що були спочатку невідомі в ньому. Це незрівнянний тому, що функціонування з прив'язаними компонентами невідомо;

• зараження вірусом – це одноразовий вплив на програми або дані, в яких вони змінюються, і, крім того, при зверненні до них виникають подібні зміни в інших, як правило, подібних компонентах: виникає «ланцюгова реакція», вірус поширюється в комп’ютерні або локальні мережі.

Назавжди довжини розрізнений визначається як тип ненавмисного впливу, і коли речей об'єкта інформації ресурсів був сприйнятий до нього.

Можливими основними цілями впливу можуть бути:

• мережеві операційні системи (SOS) та ОС комп'ютерів кінцевих користувачів (на даний момент вони сертифіковані на певний клас захисту, що передбачає вимогу самозахисту від змін);

• сервісні, реєстраційні таблиці та файли обслуговування мережі (це файли паролів, прав доступу користувачів до ресурсів, обмежень за часом і функціями тощо), програм та таблиць шифрування інформації;

• спеціальні таблиці та файли для доступу до даних на комп'ютерах кінцевих користувачів (паролі для файлів чи архівів, окремі таблиці для шифрування/дешифрування даних, таблиці ключів тощо);

• прикладні програми на мережевих комп'ютерах та їх таблиці налаштування;

• інформаційні файли комп'ютерів у мережі, бази даних, бази знань, текстові документи, електронна пошта тощо;

• параметри функціонування мережі - її продуктивність, пропускна здатність, показники часу обслуговування користувачів.

Ознаками можливого несанкціонованого впливу на мережу, що супроводжується погіршенням цих параметрів, є: уповільнення обміну інформацією в мережі, поява надзвичайно великих черг на обслуговування запитів користувачів, різке збільшення мережевого трафіку або чітко переважаючий час завантаження серверного процесора будь-яким конкретним процесором. Усі ці ознаки можна виявити та обслуговувати лише за умови ретельного аудиту та постійного моніторингу мережі.

Основними джерелами навмисного проникнення в мережу є:

• хакери (мережеві кракери), в діях яких майже завжди присутній склад злочину. Найнебезпечнішими є добре сформовані та добре організовані віртуальні хакерські групи;

• звільнених або ображених працівників мережі. Вони становлять особливу небезпеку і здатні завдати значної шкоди (особливо це стосується мережевих адміністраторів), оскільки володіють знаннями мережі та принципів інформаційної безпеки, а також мають доступ до програм для перехоплення паролів та імена користувачів у мережі, ключі, пакети тощо тощо);

• професійні мережеві спеціалісти, що займаються промисловим шпигунством;

• конкуренти, ступінь небезпеки яких залежить від цінності інформації, до якої здійснюється несанкціонований доступ, та від рівня їх професіоналізму.

Нейтралізація загроз безпеки здійснюється службами безпеки (СБ) мережі та механізмами реалізації функцій цих служб.

Наступні служби безпеки визначені документами Міжнародної організації зі стандартизації (ISO).

1. Аутентифікація (підтвердження автентичності) - забезпечує підтвердження або спростування того факту, що об'єкт, який пропонує себе як відправника повідомлення (джерела даних), є абсолютно однаковим як на етапі встановлення зв'язку між абонентами, так і на етапі повідомлення. спосіб передавання.

2. Забезпечення цілісності переданих даних - виявляє спотворення в переданих даних, вставки, повтори, знищення даних. Цей сервіс має модифікації та відмінності залежно від того, в яких мережах (віртуальних чи дейтаграмних, для цих мереж див. п. 4.8), які дії виконуються при виявленні аномальних ситуацій (з відновленням даних чи без), яке покриття переданих даних дані (повідомлення або дейтаграма в цілому або їх частини, які називаються користувацькими полями).

3. Класифікація даних - забезпечує таємність переданих даних: у віртуальних мережах - ціле передане повідомлення або тільки його виділені поля, в дейтаграмі - кожна дейтаграма або лише окремі її елементи. Служба класифікації потоку даних (трафіку), звичайна для віртуальних і дейтаграмних мереж, запобігає можливості отримання інформації про абонентів мережі та характер використання мережі.

4. Контроль доступу - забезпечує нейтралізацію спроб несанкціонованого використання спільних мережевих ресурсів.

5. Захист від відмов - нейтралізує загрози відмов від інформації з боку її відправника та/або одержувача.

Перші три сервіси характеризуються відмінностями для віртуальних і дейтаграмних мереж, а останні два сервіси є інваріантними щодо цих мереж.

Механізми реалізації функцій цих систем безпеки представлені відповідними, переважно програмними засобами. Розрізняють такі механізми: шифрування, цифровий підпис, контроль доступу, забезпечення цілісності даних, забезпечення аутентифікації, підміна трафіку, контроль маршрутизації, арбітраж. Деякі з них використовуються для реалізації не однієї, а кількох систем безпеки. Це включає шифрування, цифрові підписи, цілісність даних та керування маршрутизацією.

Використання механізмів шифрування пов'язане з необхідністю створення спеціального сервісу для генерування ключів і їх розподілу серед абонентів мережі.

Механізми цифрового підпису засновані на асиметричних алгоритмах шифрування. Вони включають процедури формування підпису відправником та його ідентифікації (перевірки) одержувачем.

Механізми контролю доступу, що реалізують функції однієї і тієї ж системи безпеки, різноманітні. Вони перевіряють повноваження користувачів і програм на доступ до мережевих ресурсів.

Механізми забезпечення цілісності даних, реалізуючи функції однойменних сервісів, виконують взаємопов'язані процедури шифрування та дешифрування даних відправника та одержувача.

Механізми аутентифікації, які на практиці зазвичай поєднуються з шифруванням, цифровим підписом і арбітражем, реалізують односторонню або взаємну аутентифікацію, коли підпис перевіряється або одним із взаємодіючих однорангових, або взаємний.

Механізми заміщення трафіку, що використовуються для реалізації послуги шифрування потоків даних, засновані на генерації фіктивних блоків, їх шифруванні та передачі по каналах зв'язку. Це ускладнює і навіть нейтралізує можливість отримання інформації про абонентів мережі та характер інформаційних потоків у ній.

Елементи керування маршрутизацією забезпечують вибір безпечних, фізично надійних маршрутів для передачі конфіденційної інформації.

Арбітражні механізми забезпечують підтвердження третьою стороною (арбітром) характеристик даних, що передаються між абонентами мережі.

1.2 Аналіз основних загроз комп'ютерних мереж

Мережева атака – це спроба отримати несанкціонований доступ до мережі організації з метою крадіжки даних або виконання інших зловмисних дій.

Існує два основних типи мережевих атак:

Пасивний: зловмисники отримують доступ до мережі та можуть відслідковувати або викрадати конфіденційну інформацію, але без будь-яких змін у даних, залишаючи їх недоторканими.

Активний: зловмисники не лише отримують несанкціонований доступ, але й змінюють дані, видаляючи, шифруючи або іншим чином ушкоджуючи їх.

Відрізняються мережеві атаки від кількох інших типів атак:

Атаки на кінцеві точки - отримання несанкціонованого доступу до пристроїв, серверів або інших кінцевих точок, як правило, їх компрометація шляхом зараження шкідливим ПЗ.

Атаки шкідливого ПЗ - зараження ІТ-ресурсів шкідливим ПЗ, що дозволяє зловмисникам зламати системи, вкрасти дані та завдати шкоди. До них також належать атаки програм-вимагачів.

Вразливості, експлойти та атаки - використання вразливостей у програмному забезпеченні, що використовується в організації, для отримання несанкціонованого доступу, злому чи саботажу систем.

Просунуті постійні загрози - це складні багаторівневі загрози, які включають мережеві атаки, а також інші типи атак.

При мережній атаці зловмисники зосереджені на проникненні через периметр корпоративної мережі та отримання доступу до внутрішніх систем. Дуже часто, опинившись усередині, зловмисники поєднують інші типи атак, наприклад, компрометація кінцевої точки, поширення шкідливого ПЗ або використання вразливості в системі мережі.

Які найпоширеніші типи мережевих атак?

Нижче наведено поширені вектори загроз, які зловмисники можуть використовувати для проникнення вашої мережі.

1. Несанкціонований доступ

Несанкціонований доступ означає, що зловмисники отримують доступ до мережі без дозволу. Серед причин атак несанкціонованого доступу – слабкі паролі, відсутність захисту від соціальної інженерії, раніше зламані облікові записи та внутрішні загрози.

2. Розподілені атаки типу "відмова в обслуговуванні" (DDoS).

Зловмисники створюють бот-мережі, великі групи зламаних пристроїв і використовують їх для направлення помилкового трафіку у вашу мережу або сервери. DDoS може відбуватися на мережевому рівні, наприклад, шляхом надсилання величезних обсягів пакетів SYN/ACC, які можуть перевантажити сервер, або на рівні програми, наприклад, шляхом виконання складних SQL-запитів, що ставлять базу даних на коліна.

3. Атакує людина посередині.

Атака "людина посередині" полягає в тому, що зловмисники перехоплюють трафік між вашою мережею та зовнішніми сайтами або всередині вашої мережі. Якщо

протоколи зв'язку не захищені або зловмисники знаходять спосіб обійти цю безпеку, вони можуть вкрасти дані, отримати облікові дані користувача і захопити свої сеанси.

4. Атаки з використанням коду та SQL-ін'єкції

Багато веб-сайтів приймають дані, що вводяться користувачем, і не можуть перевіряти і дезінфікувати ці дані. Потім зловмисники можуть заповнити форму або викликати API, передавши шкідливий код замість очікуваних значень даних. Код виконується на сервері та дозволяє зловмисникам його скомпрометувати.

5. Підвищення привілеїв

Як тільки зловмисники проникають у вашу мережу, вони можуть використати підвищення привілеїв, щоб розширити своє охоплення. Горизонтальна ескалація привілеїв передбачає, що зловмисники отримують доступ до додаткових суміжних систем, а вертикальна ескалація означає, що зловмисники одержують вищий рівень привілеїв тих самих систем.

6. Інсайдерські загрози

Мережа особливо уразлива для зловмисників, які вже мають привілейований доступ до організаційних систем. Інсайдерські загрози буває складно виявити та захистити від них, тому що інсайдерам не потрібно проникати в мережу, щоб заподіяти шкоди. Нові технології, такі як користувальницька і навіть поведінкова аналітика (UEBA), можуть допомогти виявити підозрілі або аномальні поведінку внутрішніх користувачів, що може допомогти у виявленні внутрішніх атак.

Рекомендації щодо захисту мережі

Поділ мережі

Основна частина запобігання загрозам мережній безпеці - це поділ мережі на зони на основі вимог безпеки. Це можна зробити за допомогою підмереж в одній мережі або шляхом створення віртуальних локальних мереж (VLAN), кожна з яких поводиться як повністю окрема мережа. Сегментація обмежує потенційну дію атаки однією зоною і вимагає від зловмисників вживання спеціальних заходів для проникнення в інші зони мережі та отримання доступу до них.

Регулювання доступ до Інтернету через проксі-сервер

Не дозволяти користувачам мережі виходити в Інтернет без прапорця. Передайте всі запити через прозорий проксі-сервер та використовуйте його для керування та відстеження поведінки користувачів. Переконайтеся, що вихідні з'єднання фактично виконуються людиною, а не роботом або іншим автоматизованим механізмом. Внесіть домени в білий список, щоб корпоративні користувачі могли отримувати доступ лише до явно схвалених веб-сайтів.

Правильне розміщення пристроїв безпеки

Встановіть брандмауер на кожному стику мережевих зон, а не лише на межі мережі. Якщо ви не можете повсюдно розгорнути повноцінні брандмауери, використовуйте вбудовані функції брандмауера ваших комутаторів і маршрутизаторів. Розгортайте пристрої захисту від DDoS-атак або хмарні послуги на межі мережі. Уважно продумайте, де розмістити стратегічні пристрої, такі як балансувальники навантаження - якщо вони знаходяться за межами демілітаризованої зони (DMZ), вони не будуть захищені вашим пристроєм мережної безпеки.

Використати трансляцію мережевих адрес

Трансляція мережних адрес (NAT) дозволяє перетворювати внутрішні IP-адреси на адреси, доступні в загальнодоступних мережах. Ви можете використовувати його для підключення декількох комп'ютерів до Інтернету за допомогою однієї IP-адреси. Це забезпечує додатковий рівень безпеки, оскільки будь-який вхідний або вихідний трафік повинен проходити через пристрій NAT, а IP-адрес менше, що ускладнює розуміння зловмисниками, до якого хосту вони підключаються.

Моніторинг мережевого трафіку

Переконайтеся, що у вас є повна видимість вхідного, вихідного та внутрішнього мережевого трафіку з можливістю автоматичного виявлення загроз та розуміння їхнього контексту та впливу. Об'єднайте дані з різних інструментів безпеки, щоб отримати чітке уявлення про те, що відбувається в мережі, враховуючи, що багато атак охоплюють кілька IT-систем, облікових записів користувачів та векторів загроз.

Досягнення такого рівня видимості може бути ускладнене традиційними інструментами безпеки. Cynet 360 - це інтегроване безпекове рішення, що пропонує розширену мережеву аналітику, яка безперервно відстежує мережевий трафік, автоматично виявляє шкідливу активність і або автоматично реагує на неї, або передає контекстну інформацію персоналу служби безпеки.

Використовуйте технологію обману

Ніякі заходи захисту мережі не є 100% успішними, і зловмисникам врешті-решт вдасться проникнути у вашу мережу. Усвідомте це та використовуйте технологію обману, яка створює пастки у вашій мережі, спокушаючи зловмисників «атакувати» їх та дозволяючи вам спостерігати за їхніми планами та методами. Ви можете використовувати пастки для виявлення загроз на всіх етапах життєвого циклу атаки: файли даних, облікові дані та мережеві підключення.

1.3. Причини та джерела мережевих аномалій

Щоб своєчасно запобігти атакам і забезпечити безпеку та стабільність мережі організації, необхідно регулярно контролювати стан мережі та контролювати появу мережевих аномалій, оскільки вони є однією з основних ознак збоїв у мережі та/ або зловмисник. Аналізуючи причини, джерела та ступінь небезпеки аномалії мережі, можна вчасно виявити порушення та зменшити ризики від його наслідків. Аналіз літературних джерел показує, що аномалії мережі можуть виникати з причин, пов’язаних із діяльністю зловмисників, некомпетентністю та помилками користувача, несправністю обладнання, пошкодженням каналів зв’язку та дефектами програмного забезпечення. Існують видимі аномалії, що проявляються в некоректній роботі інформаційно-обчислювальної системи в поточний момент і аномалії, які не мають видимих ознак на поточний момент, але які можуть призвести до збоїв через значний час. У цьому випадку найбільш небезпечними є аномалії, що виникають в результаті мережевої атаки. У цьому випадку метою будь-якої мережевої атаки є вторгнення

зловмисника в систему та отримання доступу до конкретних даних або ресурсу. Тому мережеві атаки можуть здійснюватися в кілька етапів і відрізнятися різним рівнем складності. Наприклад, одні види атак вимагають великої кількості обчислювальних ресурсів і високого рівня підготовки зловмисника, інші може здійснити звичайний користувач, який навіть не знає, які наслідки може призвести його діяльність. Тому, щоб мінімізувати шкоду від можливого проникнення в систему та своєчасно запобігти атаці на ранніх стадіях атаки, важливо чітко визначити ознаки атаки у виявленій аномалії та оцінити можливі наслідки. У таблиці 1 показано розвинений причинно-наслідковий зв'язок між шкідливими атаками, мережевими аномаліями та їх наслідками для безпеки мережі організації.

Таблиця 1.1.

Причини і наслідки виникнення аномалій в мережевому трафіку, джерелом яких є активність зловмисника

Причина виникнення аномалії (джерело)	Вид прояву аномалії	Наслідки
Атаки на рівні додатків	експлуатація відомих вразливостей та помилок у програмному забезпеченні, сканування та доступ до портів, асоційованих з уразливими програмами	зловмисники можуть отримати доступ до АРМ користувача мережі, підвищити привілеї, отримати адміністративний доступ

Продовження таблиці 1.1.

Авторутери	скачок у трафіку по потоках/с, з кількома пакетами в потоках від однієї домінуючої IP-адреси	установка rootkit та використання системи для автоматизації процесу вторгнення, дозволяє зловмиснику просканувати сотні тисяч систем за короткий проміжок часу
Атаки типу «відмова в обслуговуванні» (DoS) і «розподілена відмова в обслуговуванні» (DDoS)	спостерігається інтенсивний потік трафіку з безлічі IP-адрес на порти маршрутизаторів та серверів	відбуваються порушення нормального функціонування системи, порушується доступність даних та сервісів, які зазвичай доповнюються нестачею ресурсів, необхідних роботи мережі, операційної системи чи додатків
TCP SYN Flood	створення великої кількості частково відкритих з'єднань, збільшення числа SYN-пакетів	порушення нормального функціонування системи

Продовження таблиці 1.1.

Атаки "Ping of Death"	отримання надто великих IP-пакетів	збій, відмова, зависання та перезавантаження системи
Tribe Flood Network (TFN) і Tribe Flood Network 2000 (TFN2K)	генерація пакетів із підміненими IP-адресами джерела, динамічна зміна розмірів пакетів, IP-адрес та портів джерела, поява в трафіку великої кількості пакетів на одну IP-адресу	є розподіленими інструментальними засобами зазвичай запускають скоординовані DoS-атаки з багатьох джерел на одну або кілька цілей
Stacheldraht	поява нелегального зашифрованого трафіку,генерація пакетів з підміненими IP-адресами джерела, динамічна зміна розмірів пакетів, IP-адрес та портів джерела, поява в трафіку великої кількості пакетів на одну IP-адресу	відбувається вторгнення у велику кількість систем для подальшого використання їх при атаці . Потім слідує фаза DoS-атаки, протягом якої захоплені системи використовуються для атаки на один або кілька об'єктів

Продовження таблиці 1.1.

Атаки «IP spoofing»	підміна IP-адрес джерела на адреси з довірених зон	зловмисник усередині мережі або за її межами видає себе за комп'ютер, якому можна довіряти
Атаки «Man-in-the-middle»	спотворення даних, що передаються, і включення нової інформації в мережеві сесії	крадіжка інформації, хакінг поточного сеансу зв'язку для отримання доступу до приватних мережевих ресурсів, аналіз трафіку — для отримання інформації про мережу та її користувачів, DoS-атаки, спотворення даних, що передаються, і включення нової інформації в мережеві сесії
Мережна розвідка	запити до DNS-серверу, сканування діапазону IP-адрес (ping sweeps) та сканування портів	зловмисники можуть знайти відкриті порти, вивчити характеристики програм, що виконуються на хостах

Продовження таблиці 1.1.

Сніффінг пакетів	перехоплення пакетів, що передаються по мережі у відкритому вигляді (служби telnet, FTP, SMTP, POP3 і т. д.), наприклад імен користувачів та паролі, перемикання потоків трафіку з одного мережного пристрою (служби) на інше	зловмисник може отримати доступ до облікової записи системного користувача, який хакер може використовувати для створення нового облікового запису, і таким чином мати доступ до мережі та її ресурсів у будь-який час
Атаки на паролі	підробка IP-пакетів та прослуховування пакетів, скачок у трафіку по потоках/с, з кількома пакетами від однієї домінуючої IP-адреси	зловмисники можуть забезпечити собі вхід до мережі, незалежно від можливих майбутніх змін зламаних даних
Port redirection attacks	переадресація мережевого трафіку, падіння в байтах або пакетах в одному потоці трафіку і викид в іншому	Передача зловмисниками через міжмережевий екран нелегального трафіку

Продовження таблиці 1.1.

Вірусні та троянські атаки	викид у трафіку без домінуючої адреси призначення, але з одним або декількома домінуючими портами призначення	прикладом вірусу є програма, яка видаляє деякі мережеві файли та інфікує всі інші версії файлу command. com, які можна знайти.
Trust exploitation attacks	відбуваються, коли хтось користується перевагою довірчих відносин у межах мережі	атака на внутрішню мережу

2 АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП’ЮТЕРНИХ МЕРЕЖ ВІД АНОМАЛІЙ

2.1. Аналіз аномалій мережевого трафіку комп’ютерних мереж

Проблеми у комп'ютерних мережах визначаються як аномалії трафіку, що вони викликають. Загалом, аномалія - те, що суперечить очікуванням. Наприклад, пошкоджений комутатор може створити несподіваний трафік в іншій частині мережі або що нові коди помилок починають з'являтися, коли служба не працює. Виправлення неполадок у мережі базується на аномаліях мережі.

Перший метод класифікації аномалій ґрунтується на тому, чим вони відрізняються від звичайного спілкування. Аномалії можуть відрізнятися за типом даних (поведінкові), за обсягом переданих даних (за обсягом) або за обома критеріями. Інший спосіб класифікації аномалій - з їхньої причини:

Помилка, не пов'язана з людським фактором - наприклад, відмови обладнання або радіозв'язок, перервана погодними умовами;

Людська помилка - наприклад, збій мережевих послуг через неправильну конфігурацію або випадкове відключення мережного кабелю;

Шкідлива діяльність людини - наприклад, інсайдерська атака, коли незадоволений співробітник компанії ушкоджує мережевий принтер, або зовнішня атака, коли зловмисник намагається вивести з ладу мережу та завдати шкоди репутації.

Що таке система виявлення аномалій?

Виявлення аномалій потребує постійного моніторингу та аналізу вибраних мережевих показників. Система виявлення аномалій охоплює сценарій, коли виявляється щось несподіване і аналіз оцінює це як аномалію, про це можна повідомити адміністратору мережі.

Існує дві основні категорії мережного моніторингу, що дозволяють виявляти аномалії:

Пасивний моніторинг мережі

Комп'ютерна мережа включає зонди, які отримують дані з мережі та оцінюють їх. Ці дані можуть бути призначені безпосередньо для зондів (наприклад, події, відправлені за протоколом SNMP), або вони можуть бути копією виробничого трафіку, який відбувається в мережі незалежно від того, підключений зонд чи ні.

Активний моніторинг мережі

Мережі можуть також містити зонди як при пасивному моніторингу, але ці зонди генерують додатковий трафік, який вони відправляють через мережу. За допомогою цього трафіку можна регулярно визначати доступність або загальні параметри сервісів, мережевих ліній і пристроїв, що тестуються.

Відмінності між активним та пасивним мережевим моніторингом при виявленні аномалій мережі

Може здатися, що активний моніторинг розширює можливості пасивного моніторингу, автоматично робить його найкращим варіантом. Проте проблема з активним моніторингом полягає в тому, що він генерує додаткові дані в мережі. Отже, при активному моніторингу пристрої моніторингу стають частиною виробничої мережі (що несе із собою, наприклад, ризики безпеки), і, отже, моніторинг не повністю прозорим. Інша потенційна проблема полягає в тому, що дані моніторингу можуть впливати на функціональність мережі і, таким чином, бути джерелом проблем і аномалій (наприклад, вони можуть збільшити навантаження на вже зайнятий сервер). Враховуючи ці недоліки, ця стаття присвячена лише пасивному моніторингу аномалій мережі.

У цілому нині виявлення аномалій можна розділити кілька основних компонентів; див. рисунок 1 (діаграма праворуч). Вони мають такі функції:

Параметризація - контрольовані дані відокремлюються від вхідних даних у формі, придатній для подальшої обробки.

Навчання – при виборі цього режиму оновлюється мережева модель (навчений статус). Це оновлення може виконуватися як автоматично, так і вручну.

Виявлення - створена (навчена) модель потім використовується для порівняння даних із відстежуваної мережі. Якщо він відповідає певним критеріям, створюється звіт про виявлення аномалії.

2.2 Аналіз методів виявленням аномалій мережі за допомогою сигнатур і базових ліній

Таблиця 2.1.

Атрибут	Сигнатури	Базові лінії
Можливість виявлення відомих помилок або атак	Високий - якщо підпис існує	Низький – відхилення від базової лінії не прив’язане до конкретної ситуації
Можливість виявлення невідомих помилок або атак	Низький – якщо для помилки чи атаки немає сигнатури, її неможливо виявити	Висока – відхилення від базової лінії не прив’язане до конкретної ситуації
Складність ведення бази знань	Високий – наявні підписи вимагають оновлення, а нові потрібно створити	Низький – базову лінію можна автоматично перерахувати з часом

Продовження таблиці 2.1.

Швидкість виявлення	Швидко – коли деякі дані відповідають критеріям виявлення, аномалія виявляється	Швидко – коли деякі дані відповідають критеріям виявлення, аномалія виявляється
Швидкість розгортання	Швидко – аномалії можна виявити відразу після розгортання	Повільно – базову лінію потрібно навчити, перш ніж вона зможе почати виявляти
Кількість хибнопозитивних виявлення	Менший — якщо сигнатури чітко визначені, звичайні пакети не відповідатимуть своїм критеріям	Більший – будь-які коливання можуть викликати аномалію

Хоча виявлення аномалій за допомогою сигнатур є швидким і точним, воно може працювати тільки з аномаліями трафіку, для яких сигнатура відома. З іншого боку, виявлення на основі машинного навчання відбувається повільніше і виявляє більше помилкових спрацьовувань, але здатне виявити нові та змінені аномалії, для яких не існує сигнатури. Як правило, неможливо виявити всі аномалії, не виявивши помилкових спрацьовувань. Тому рекомендується збалансований підхід.

Використання машинного навчання для виявлення аномалій

Щоб сигнатури були точними та дозволяли виявляти відомі аномалії в мережі, їх необхідно створювати вручну з урахуванням кожної проблеми чи атаки. З іншого боку, базові рівні можуть використати алгоритми машинного навчання. Основна

перевага використання машинного навчання полягає в тому, що базовий рівень може змінюватися з часом, залежно від того, які дані були фактично виявлені, що дозволяє отримувати уроки з попередніх результатів.

Алгоритми машинного навчання (наприклад, евристики) використовуються системами виявлення вторгнень на основі аномалій, які працюють за принципом відхилень від вивченої норми.

Перевага використання машинного навчання полягає в тому, що методи рідко вимагають будь-яких знань про відстежувану мережу, але вони все ж таки можуть вивчити очікувану поведінку і виявляти аномалії. Однак є зворотний бік: якщо помилка проявляється у поступовому збільшенні певних атрибутів, жодних аномалій не виявлено. Натомість вивчена модель повільно пристосовуватиметься до нового збільшення цих атрибутів, і виявлення не відбудеться. Витончена атака може скористатися цим, щоб уникнути виявлення.

Проблеми з виявленням аномалій

Реальність виявлення аномалії не така проста, як може здатися. Зрештою, виникне проблема, яка суттєво обмежить можливості виявлення аномалій. У цьому розділі описано дві найважливіші проблеми.

Неправдиве виявлення

Не завжди легко відрізнити нормальну роботу від аномалії. Те, що вчора могло бути нормальним рухом, завтра може стати аномалією. Це з тим, що передані дані змінюються незалежно від цього, є проблема (аномалія) у мережі чи ні. Ось чому виявлення швидше працює із оцінками ймовірності. Хоча кожна система або метод може використовувати його по-різному, основна ідея та сама. Кожній виявленій події надається оцінка, і якщо ця оцінка перевищує заздалегідь встановлений поріг, вона відзначається як аномалія.

Порог виявлення аномалій визначає чутливість виявлення. Якщо чутливість занадто висока, проблеми або аномалії будуть виявлені швидко, але за рахунок збільшення кількості подій, які помилково помічені як аномальні. Ці неправильно

марковані події називаються хибними спрацьовуваннями. З іншого боку, якщо чутливість низька, кількість помилкових спрацьовувань зменшується, але водночас зменшується кількість правильно виявлених аномалій - аномалія деяких аномалій буде недостатньо високою, що дозволяє залишатися непоміченими.

Прикладом неправдивої події є випадок, коли несподіване оновлення операційної системи передає великий обсяг даних, або коли несподівана обставина спонукає ненормальну кількість клієнтів одночасно підключитися до інтернет-магазину компанії.

Взагалі кажучи, неможливо гарантувати, що всі аномалії в мережі будуть виявлені і водночас не будуть помилковими спрацьовуваннями. Причина, через яку помилково позитивні події насправді є проблемою, полягає в тому, що під час автоматичної обробки подій законний трафік або послуга можуть бути визначені як проблемні, і їхня активність буде обмежена. У той же час обробка та аналіз цих аномалій вручну потребує величезних витрат часу та зусиль.

Моніторинг зашифрованого трафіку ускладнює виявлення застарілих аномалій

З міркувань конфіденційності та безпеки в комп'ютерних мережах шифрування даних розширюється та покращується. Зашифрований зв'язок також впливає на виявлення аномалій, оскільки шифрування даних зменшує обсяг даних, з якими можуть працювати моніторинг та аналіз. Наприклад, під час моніторингу зашифрованої електронної пошти адреси електронної пошти недоступні.

Важливо знати, якому рівні відбувається шифрування. Більшість обміну даними шифрується тільки на рівні програми, що означає, що, як і раніше, можна виконувати статистичний аналіз IP-адрес, портів призначення і т. д. Таким чином, шифрування не запобігає виявленню аномалій, але значно обмежує типи аномалій, які можуть бути виявлено. На жаль, зловмисники та різні шкідливі скрипти також знають про цей факт та приховують свою діяльність у зашифрованому повідомленні, щоб уникнути виявлення.

2.2.1. Опис системи моніторингу

Початковим завданням у створенні системи моніторингу було визначення архітектури системи, її компонентів та схеми взаємодії між ними. Використовується клієнт-серверна архітектура, що сприяє незалежності компонентів та створенню розподіленої системи.

Архітектура системи включає наступні компоненти:

Мережевий сенсор перехоплює вхідний трафік і сортує за протоколами з підрахунком кількості пакетів, їх довжин, прапорів та інших параметрів. Сенсор пов'язаний з сегментом локальної мережі для перехоплення трафіку, базою даних для читання правил розбору пакетів та аналізатором для передачі статистики.

Модуль-аналізатор отримує дані про мережевий трафік від сенсора і розраховує метрики – показники інтенсивності аномалії. Далі аналізатор перевіряє критерії наявності аномалії та при необхідності викликає модуль відповіді для реакції.

База даних є реляційною. Для створення бази даних використовувалася СУБД MySQL. База даних розбита на 3 частини, які можуть бути реалізовані на окремих серверах:

1) описова частина зберігає інформацію про протоколи, що вимірюються ознаками, метриками, критеріями аномалій;

2) статистичні дані щодо вимірюваних величин – таблиці з даними за протоколами, метриками, подіями про загрози;

3) адміністративна частина зберігає інформацію про користувачів системи.

Модуль прогнозу є опціональним та використовує моделі побудови профілю мережевої активності та прогнозування часових рядів.

Модуль відповіді призначений реакцію наявність аномалії. Реакція ґрунтується на даних, які від аналізатора.

Веб-інтерфейс розроблений для візуалізації та адміністрування системи моніторингу, за допомогою нього можна переглянути всі події по загрозах, весь вхідний трафік за певний період, за певними протоколами як реального часу.

Для адміністратора існує налаштування бази даних, відображених протоколів, подій, пов'язаних із загрозами.

2.2.2. Аналіз обробки даних в мережевому трафіку

Обробка даних у системі відбувається у ряд етапів .

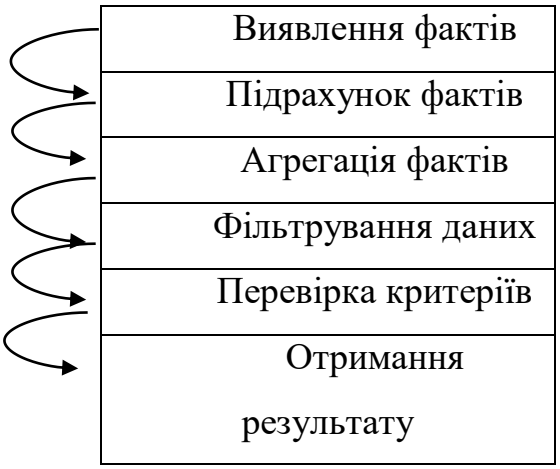

Рис. 2.1. Етапи обробки даних у системі

Виявлення фактів являє собою виділення з мережевого трафіку пакетів, що мають значущі для виявлення ознаками (наприклад, пакети, відповідні певному протоколу; пакети з деяким значенням поля або прапора в заголовку).

Підрахунок фактів є обчисленням кількості та/або обсягу пакетів для кожної ознаки, що враховується на попередньому етапі обробки даних.

Агрегація фактів – визначення кількості та/або обсягу пакетів для кожної ознаки за період.

Фільтрування даних полягає у застосуванні статистичних методів для ослаблення впливу випадкових варіацій у часових лавах. Застосовуються методи виділення тренду, наприклад метод ковзного середнього.

Перевірка критеріїв полягає в побудові списку критеріїв аномалій мережі, що виконуються в даний момент. Критерії визначаються пороговими значеннями вимірюваних величин.

Отримання результату є визначення типів аномалії виходячи з отриманої на попередньому етапі комбінації атак.

2.3. Аналіз статистичні методи виявлення аномальної поведінки

Основний недолік методів виявлення мережевих атак на основі сигнатур, пов'язаний з нездатністю системи виявляти атаки невідомого типу. Це можна усунути шляхом застосування методів на основі виявлення аномалій у мережевій активності. Такі методи засновані на припущенні, що для обчислювальної системи існує профіль нормального стану і будь-які значні відхилення від нього є ймовірним кандидатом для можливої атаки. Основною перевагою цього методу є можливість виявлення нових, раніше невідомих типів атак. Для побудови базового профілю системи використовується набір даних, вільний від аномалій, або статистичні методи.

Як клас, статистичний аналіз відноситься до поведінкових

методів виявлення збоїв у роботі мережі та ґрунтується на порівнянні поточного стану мережевої інфраструктури з певними заздалегідь визначеними ознаками, що характеризують нормальне функціонування мережевої інфраструктури. Методи статистичного аналізу мають різні інтерпретації, засновані на різних динамічних характеристиках мережевого трафіку, але основні принципи майже ідентичні для всіх. Безперечною перевагою використання методів статистичного аналізу є можливість вперше визначити реалізовані методи негативного впливу на об'єкт атаки з боку зловмисника. Однак для її успішної реалізації необхідно визначитися з об’єктом

аналізу, мають певні структуровані характеристики, які формують правильну конфігурацію, і критерії, за якими можна визначити потенційну загрозу безпеці мережі.

Використання методів статистичного аналізу є найбільш поширеною реалізацією технології виявлення аномальної поведінки. Статистичні датчики збирають різну інформацію про типову поведінку об'єкта і формують її у вигляді

профілю. Профіль у цьому випадку — це набір параметрів, що характеризують типову поведінку об’єкта. Настає період формування початкового профілю. Профіль формується на

статистику об’єктів, а також можна використовувати стандартні методи математичної статистики, такі як ковзні вікна та зважені суми. Статистичні методи універсальні, оскільки аналіз не вимагає знання

можливі атаки та вразливості, які вони використовують, і засновані на змінах деяких статистичних характеристик потоку пакетів. Для використання статистичних методів для аналізу трафіку TCP/IP необхідно виділити основні показники, що характеризують

регулярну експлуатацію мережевої інфраструктури, а також здійснювати динамічний контроль за їх станом. В якості таких індикаторів слід використовувати інформацію, яка може бути використана для аналізу історії мережевої взаємодії. Дані, які можна аналізувати, наприклад, при захопленні трафіку TCP/IP, включають поля заголовків протоколів IP, TCP, UDP, ICMP і вміст полів даних.

Після формування профілю дії об’єкта порівнюються з відповідними параметрами, а при виявленні значних відхилень подається сигнал про початок атаки.

У обладнанні для моніторингу встановлюються механізми спостереження для спостереження за властивостями або поведінкою системи та для подачі сигналу тривоги, якщо важливий параметр змінюється в діапазоні чутних операцій. Виявлення таких подій часто пов'язане з виявленням значних змін нормального стану системи. Нормальний стан можна визначити специфікацією або вимірюваннями на початку та правильного калібрування системи. Існує багато можливих причин для змін, таких як несправності, поломки та знос. Незалежно від причини, часто важливо швидко виправити зміну, наприклад, відремонтувати або відкалібрувати систему, щоб уникнути пошкодження в майбутньому.

У контексті аналізу трафіку нас цікавлять методи захоплення для виявлення аномалій руху. Передбачається, що причинами аномалій руху є значні зміни деяких

характеристик руху. Однак якість результатів виявлення залежить не тільки від обраного методу виявлення змін. Ще важливіше вибрати показники розглянутого трафіку, які є найбільш чутливими до подій, пов'язаних з роботою та адмініструванням мережі, наприклад, збої в мережі, атаки шкідливого трафіку.

З іншого боку, показники повинні бути достатньо чутливими до змін трафіку та несправностей, спричинених законним і нешкідливим трафіком. Інакше ми ризикуємо отримати велику кількість помилкових і нецікавих тривог.

Особливістю знаходження змін є серія спостережень, а не конкретне значення. Усередині такого ряду зміни шукають у момент часу, коли статистичні властивості величини, що спостерігається, різко змінюються. «Різкий» означає, що зміна відбувається миттєво або, принаймні, дуже швидко протягом періоду спостереження. До і після змін статистичні властивості або не змінюються, або змінюються незначно. За цих умов можна виявити навіть невеликі та стійкі зміни, але з більшим часом затримки виявлення, ніж великі зміни. Причина більше спостереження, зібрані після зміни.

2.4. Аналіз програм для аналізу мережевого трафіку

Аналіз трафіку – це процес, про важливість якого знає будь-який IT-спеціаліст, незалежно від того, чи працює він у невеликій компанії чи великій корпорації. Адже виявлення та усунення проблем мережі – це справжнє мистецтво, яке безпосередньо залежить як від інстинкту самого фахівця, так і від глибини та якості даних, якими він оперує. А аналізатор трафіку — це саме той інструмент, який надає вам ці дані. Грамотно підібране рішення для аналізу мережевого трафіку може не тільки допомогти вам зрозуміти, як пакети надсилаються, отримуються та наскільки безпечно вони передаються по вашій мережі, але й може зробити набагато, набагато більше!

Сьогодні на ринку існує багато різновидів програмного забезпечення для аналізу мережевого трафіку. Більше того, деякі з них здатні викликати ностальгічні спогади у фахівців «старої школи»; вони використовують термінальний шрифт і інтерфейс командного рядка, і на перший погляд здаються складними у використанні. Інші рішення, навпаки, виділяються простотою монтажу і орієнтовані на аудиторію з візуальним сприйняттям (вони буквально перенасичені різноманітними графіками). Ціновий діапазон цих рішень також дуже різний – від безкоштовних до рішень з дуже дорогою корпоративною ліцензією.

Для того, щоб ви, в залежності від ваших завдань і уподобань, могли вибрати найкраще рішення для аналізу мережевого трафіку, представляємо вам список найцікавіших програмних продуктів, доступних на ринку для аналізу трафіку, а також короткий огляд вбудованої в них функціональності для вилучення, обробки та візуального представлення різноманітної мережевої інформації. Деякі з цих функцій подібні для всіх рішень для аналізу мережевого трафіку, представлених у цьому огляді – вони дозволяють бачити надіслані та отримані мережеві пакети з тим чи іншим рівнем деталізації – але майже всі вони мають деякі характерні особливості, які роблять їх унікальний при використанні в певних ситуаціях або мережевих середовищах. Зрештою, ми звертаємося до аналізу мережевого трафіку, коли маємо проблему з мережею, але не можемо швидко звести її до конкретної машини, пристрою чи протоколу, і нам доводиться проводити більш глибокий пошук. Ми допоможемо вибрати найбільш підходяще програмне рішення для аналізу трафіку для цих цілей.

SolarWinds Network Bandwidth Analyzer

Дане рішення позиціонується виробником як програмний пакет, що складається з двох продуктів - Network Performance Monitor (базове рішення) і NetFlow Traffic Analyzer (модульне розширення). Кажуть, що вони мають схожі, але все ж різні функції аналізу мережевого трафіку, які доповнюють один одного, коли два продукти використовуються разом.

Монітор продуктивності мережі, як випливає з назви, відстежує продуктивність мережі і є привабливим вибором, якщо ви хочете отримати уявлення про те, що відбувається у вашій мережі. Купуючи це рішення, ви платите за можливість відстежувати загальний стан вашої мережі: покладаючись на величезну кількість статистичних даних, таких як швидкість і надійність передачі даних і пакетів, у більшості випадків можна швидко визначити проблеми у своїй мережі. А розширений інтелект програми у визначенні потенційних проблем і широка можливість візуалізації результатів у вигляді таблиць і графіків із чіткими попередженнями про можливі проблеми ще більше полегшать цю роботу.

Модульне розширення NetFlow Traffic Analyzer більше фокусується на аналізі самого трафіку. У той час як функціональність основного програмного рішення Network Performance Monitor більше призначена для отримання уявлення про продуктивність мережі, в NetFlow Traffic Analyzer акцент зосереджений на більш детальному аналізі процесів, що відбуваються в мережі. Зокрема, ця частина програмного пакета аналізуватиме перевантаження або ненормальні стрибки пропускної здатності та надає статистику, відсортовану за користувачами, протоколами чи програмами. Зверніть увагу, що ця програма доступна лише для середовища Windows.

Wireshark

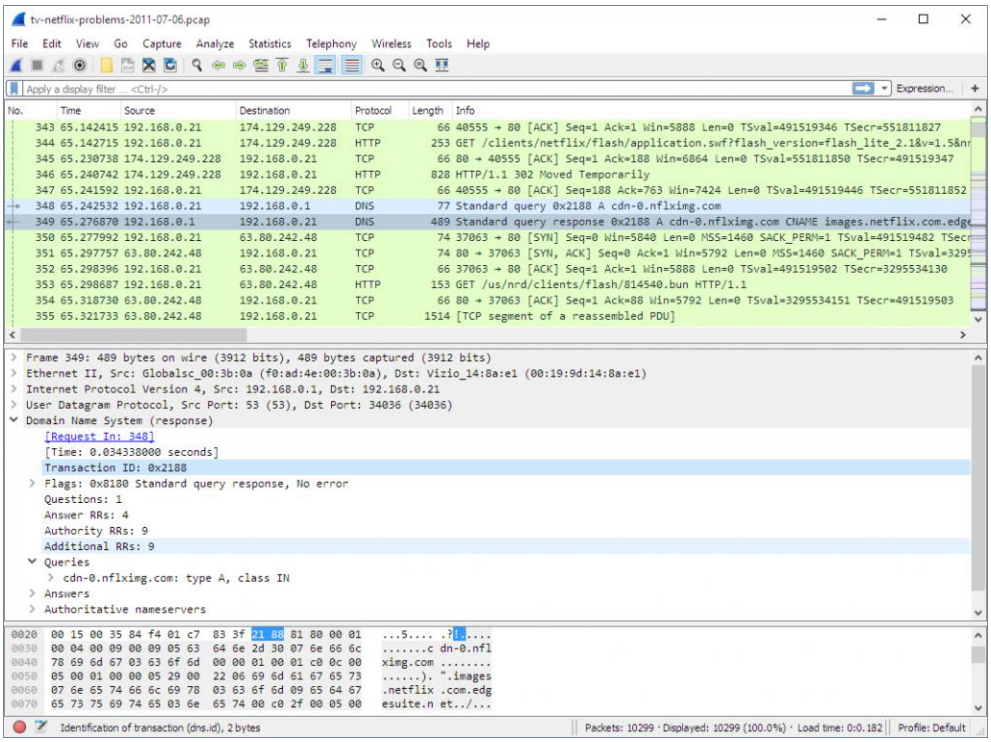

Рис. 2.2. Приклад роботи Wireshark

WireShark є відносно новим інструментом у великому сімействі рішень для діагностики мережі, але за цей час він уже здобув визнання та повагу з боку IT-фахівців. WireShark відмінно справляється з аналізом трафіку, відмінно справляючись з роботою за вас. Розробникам вдалося знайти золоту середину між вихідними даними і візуальним представленням цих даних, тому в WireShark ви не знайдете зміщення в ту чи іншу сторону, що грішать більшість інших рішень для аналізу мережевого трафіку. WireShark простий, сумісний і портативний. З WireShark ви отримуєте саме те, що очікуєте, і ви отримуєте це швидко.

WireShark має чудовий інтерфейс користувача, безліч параметрів фільтрації та сортування, і, як багато хто з нас оцінить, аналіз трафіку WireShark чудово працює з будь-яким із трьох найпопулярніших сімейств операційних систем - * NIX, Windows і macOS. Додайте до всього вищесказаного той факт, що WireShark є відкритим вихідним кодом і безкоштовним, і у вас є чудовий інструмент для швидкої діагностики вашої мережі.

tcpdump

Аналізатор трафіку tcpdump виглядає як старовинний інструмент, і, чесно кажучи, він працює так само з точки зору функціональності. Незважаючи на те, що він справляється зі своєю роботою і справляється добре, і використовуючи для цього мінімум системних ресурсів, наскільки це можливо, багатьом сучасним фахівцям буде важко розібратися у величезній кількості «сухих» таблиць з даними. Але в житті бувають ситуації, коли використання настільки відрізаних і невибагливих до ресурсів рішень може бути корисним. У деяких середовищах або на ПК, що майже не працюють, мінімалізм може бути єдиним життєздатним варіантом.

Програмне рішення tcpdump спочатку було розроблено для середовищ * NIX, але зараз воно також працює з кількома портами Windows. Він має всі основні функції, які ви очікуєте побачити в будь-якому аналізаторі трафіку - захоплення, запис тощо, але не варто вимагати від нього більше.

NetworkMiner

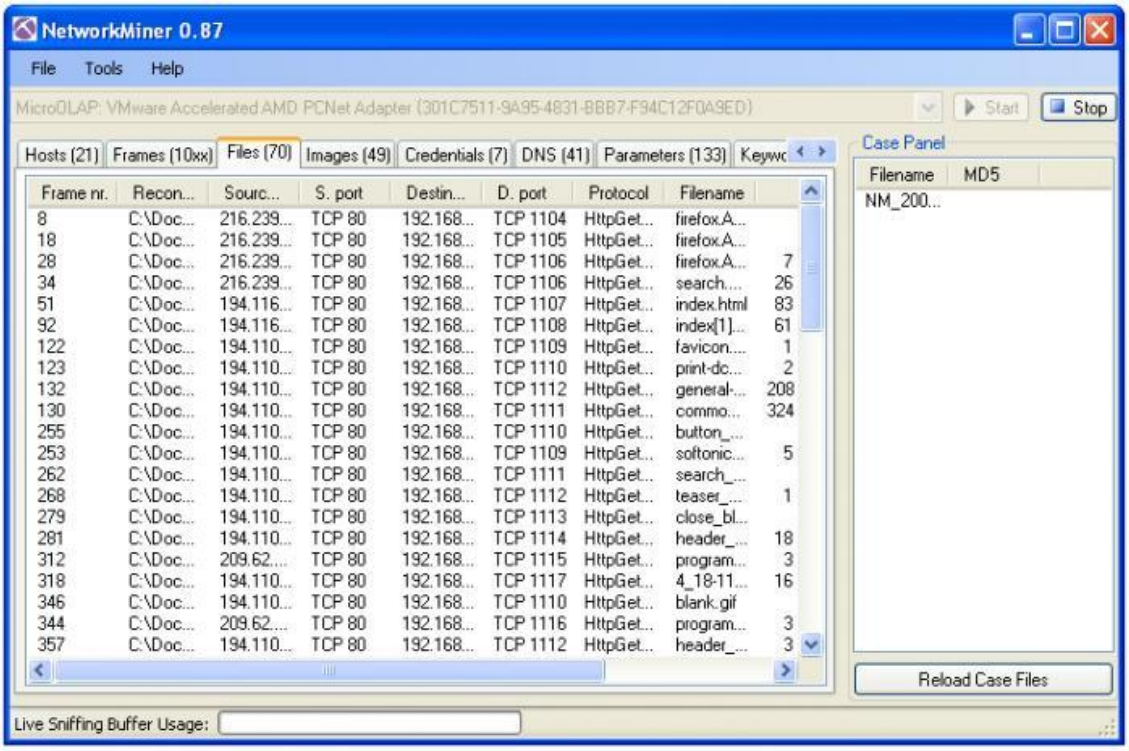

Рис.2.3 Інтерфейс рішення NetworkMiner

Рішення NetworkMiner – це ще одне програмне рішення, функціональність якого виходить за рамки звичайного аналізу трафіку. У той час як інші аналізатори трафіку зосереджуються на відправленні та отриманні пакетів, NetworkMiner відстежує, хто надсилає та отримує пакети. Цей інструмент більше підходить для виявлення проблемних комп'ютерів або користувачів, ніж для виконання загальної діагностики або моніторингу самої мережі. NetworkMiner розроблений для ОС Windows.

Cisco Stealthwatch

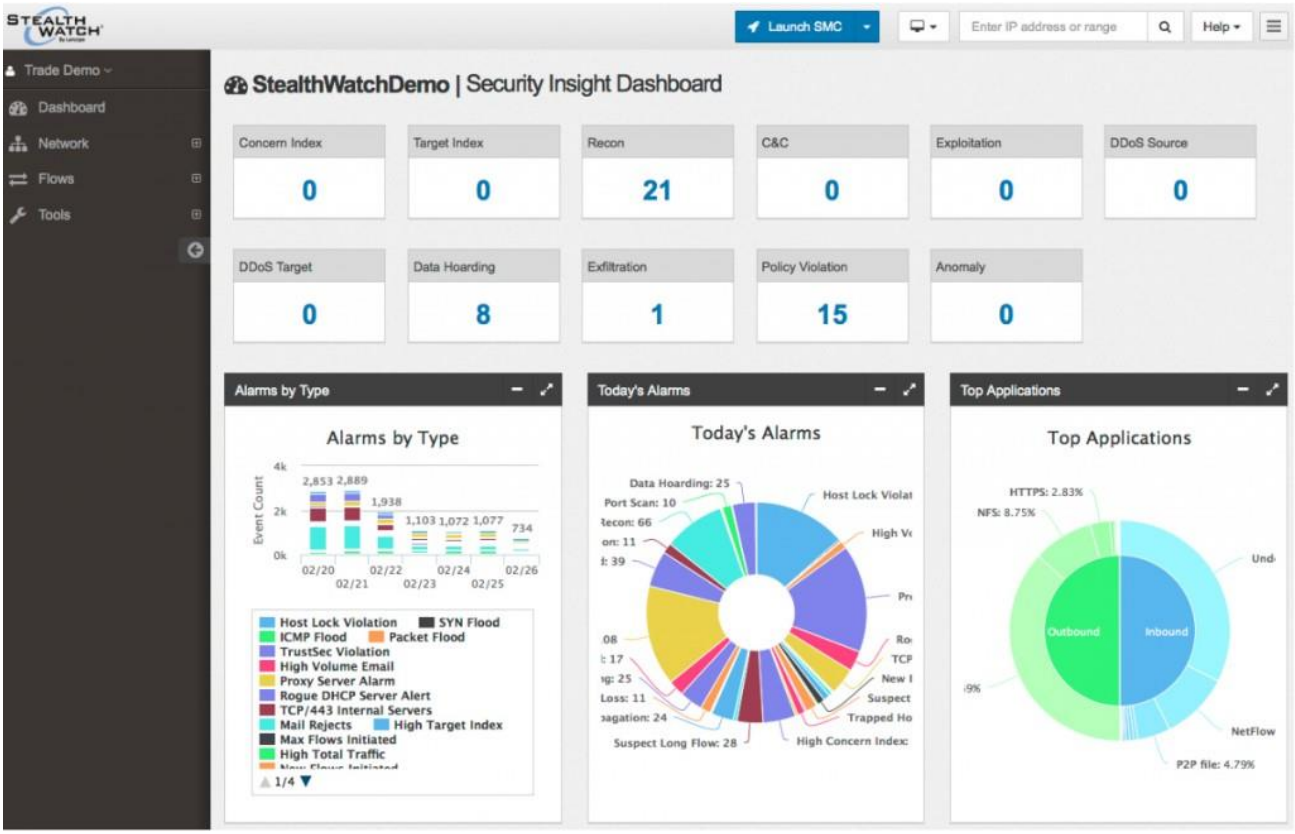

Рис. 2.4. Інтерфейс рішення Cisco Stealthwatch

Cisco Stealthwatch інтегрує та аналізує мережеву телеметрію, інформацію, створену мережевими пристроями. Ви отримуєте можливість бачити потоки системного трафіку від межі мережі до центру обробки даних, включаючи віртуальні машини. Stealthwatch виявляє широкий спектр проблем мережі та центрів обробки даних від зловмисників, які намагаються заблокувати конфіденційні дані для поширення шкідливого програмного забезпечення в організації від хоста до хоста.

3 ТЕХНОЛОГІЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

3.1. Аналіз функцій та можливостей Cisco StealthWatch

Cisco StealthWatch - це засіб забезпечення ІБ в мережі, яке засноване на зборі телеметричних даних з різних пристроїв, тобто не тільки з МСЕ, які стоять на периметрі, а також з інфраструктурних пристроїв, таких як маршрутизатори, комутатори, сервери з віртуальними машинами і навіть з призначених для користувача пристроїв (не важливо підключені вони зсередини корпоративної мережі або перебувають за її межами).

Оскільки в якості основного протоколу збору даних по телеметрії в рішенні Cisco StealthWatch є широковідомий і популярний NetFlow/IPFIX, це дозволяє обійтися без окремої виділеної фізичної мережі для моніторингу, тобто можна використовувати вже наявне мережеве обладнання. А якщо на якійсь ділянці корпоративної мережі немає пристроїв з підтримкою NetFlow, то в Cisco StealthWatch є рішення і для цього випадку.

Причому Cisco StealthWatch не просто збирає ці дані (тобто є колектором цих даних), він вміє їх дедупліцірувати, збагачувати дані телеметрії даними з інших джерел і т.д., все це формує із розрізнених джерел інформації найбільш повний контекст ІБ про потоках трафіку в корпоративній мережі, доступний в real time режимі. Розширену інформацію про контекст безпеки для Cisco StealthWatch надає інше рішення - Cisco ISE, а також хмарні служби Cisco, що містять бази даних IP / URL-репутацій).

З допомогою Cisco StealthWatch вся корпоративна мережа передачі даних трансформується в єдиний сенсор, детектующий атаки, аномальну поведінку і т.д. Це рішення виходить за межі корпоративної мережі, дозволяючи навіть моніторити

хмарні середовища і мобільних користувачів. Рішення знає все про кожен хост і користувача в мережі, записує всі його дії в мережі (в тому числі бачить мережевий трафік на рівні сигнатур додатків), відстежує відхилення від «нормальної» поведінки (причому в рішенні є можливість створення профілю «правильногї» поведінки (baseline) у вигляді механізму автонавчання), забезпечує зберігання цих даних, дозволяє робити вибірки з цих даних (включаючи аналіз підозрілої активності, так як в Cisco StealthWatch вже зашито більше 100 різних алгоритмів виявлення аномалій і поведінки), попереджає адміністраторів про будь-які зміни. Рішення можна використовувати в якості інструменту для проведення постійного аудиту працездатності традиційних засобів забезпечення ІБ, а також його корисно використовувати для розслідування шляхів поширення шкідливого коду і векторів атаки (та сама можливість «пірнути» в історичні дані).

3.2. Аналіз технологій виявлення аномалій на базі Cisco StealthWatch

По-перше, поведінкове моделювання та поведінкові сигнатури, іншими словами, постійне відстежування кожного пристрою в мережі і можливість визначати базові показники нормальної і аномального поведінки. Для кожного хоста будь то користувач, сервер або роутер будується свій baseline (ідеальна модель поведінки), відхилившись від якого ми бачимо все аномалії щодо даного хоста.

Як приклад: користувач раптом почав завантажувати великі обсяги даних, хоча він цього ніколи не робив - StealthWatch практично миттєво це визначає.

По-друге, глобальна аналітика загроз. Під цим розуміється інтеграція з відомої Cisco Talos - величезною базою даних сигнатур відомих атак, оновлюваної по всьому світу в режимі реального часу.

По-третє, старе добре машинне навчання, у випадку з Cisco засноване на технології Cognitive Intelligence.

Технологія також лежить в основі рішення ETA - Encrypted Traffic Analytics, яка дозволяє визначити погане чи зашифроване з'єднання без його розшифровки (атака, небажаний трафік і C & C комунікації).

По суті, Cisco Stealthwatch значно покращує захист від загроз, надаючи детальну видимість мережі та аналітику безпеки. Це допомагає вам знати кожного хоста, записувати кожну розмову, розуміти, що є нормальним, попереджає про зміни та дає змогу швидко реагувати на загрози. Stealthwatch застосовує машинне навчання та статистичне моделювання до мережевої телеметрії, зібраної з усієї розширеної мережі, включаючи центр обробки даних, філію, кінцеві точки та хмару .

Stealthwatch збирає телеметрію з кожної частини мережі та застосовує передову аналітику безпеки до даних. Він створює базову лінію нормальної веб- та мережевої активності для мережевого хоста та застосовує контекстно-залежний аналіз для автоматичного виявлення аномальної поведінки. Stealthwatch може ідентифікувати широкий спектр атак, включаючи шкідливе програмне забезпечення, атаки нульового дня, спроби розподіленої відмови в обслуговуванні (DDoS), розширені постійні загрози (APT) та інсайдерські загрози.

Stealthwatch також інтегровано з хмарною платформою виявлення загроз та аналітики, яка застосовує комбінацію контрольованого та неконтрольованого машинного навчання, щоб вчитися на тому, що він бачить, і адаптуватися до змінної поведінки мережі з часом. Це дійсно безпрограшний варіант.

Використовуючи Netflow та інші телеметричні дані з існуючої інфраструктури, це рішення може економічно ефективно перетворити всю мережу в систему датчиків. Рішення виявляє ненормальний трафік і поведінку, включаючи зловмисне програмне забезпечення нульового дня, атаки розподіленої відмови в обслуговуванні (DDoS), внутрішні загрози та новітні цільові загрози (APT). Stealthwatch має інтуїтивно зрозумілий веб-інтерфейс. Він забезпечує єдине уявлення про горизонтальний рух трафіку в мережі. Крім того, система забезпечує високотехнологічний аналіз і

оповіщення. Ця проста, легка у використанні та потужна платформа розширює ваші можливості щодо використання, аналізу безпеки та раннього виявлення загроз.

Cisco Stealthwatch

Cisco Stealthwatch об'єднує та аналізує сетеву телеметрію, інформацію, генеруючу сетевими пристроями. Ви отримуєте видимість у потоках системного трафіку від мережі периметра до центру обробки даних, включаючи віртуальні машини. Stealthwatch виявляє широкий спектр проблем, пов'язаних із сетями й центрами обробки даних, від шкідливих інсайдерів, які намагаються перекрити конфіденційні дані для поширення шкідливого ПО всередині організації з хоста. Він працює з усіма маршрутизаторами та коммутаторами Cisco, а також з різними рішеннями безпеки:

- Захищений центр обробки даних Cisco
- Гнучкий NetFlow Cisco IOS
- Технологія безпеки Cisco TrustSec
- Cisco ASA з FirePOWER Services (NGFW)
- Cisco Identity Services Engine (ISE)
- Cisco Web Security Appliance (WSA)
- Аналізатор пакетів безпеки Cisco
- Переваги Cisco Stealthwatch

Stealthwatch використовує мережеві дані для прискорення та покращення виявлення аномалій, реагування на інциденти та їх розслідування у всій вашій мережі. Він встановлює базовий рівень того, що вважається нормальною поведінкою та активністю у мережі. З цією базою як основна точка відліку ви можете використовувати це рішення для виявлення аномальної поведінки у вашій мережі, яке може означати атаку. Пропоноване рішення використовує потоки трафіку для

моніторингу всього вашого середовища, щоб визначити, чи відбуваються порушення політик безпеки та мережного доступу.

Пропоноване рішення постійно відслідковує рух у мережі з північ-південь і схід-захід всередині вашої мережі, щоб визначити трафік, який може сигналізувати про зловживання системою та загрози інсайдера. Це дозволяє вам допомагати виявляти та захищати від шкідливих програм Zero-day, APT, спроб DDoS та інших атак, перш ніж вони завдадуть шкоди. Консоль управління Stealthwatch дозволяє переглядати та відстежувати ці потоки трафіку для виявлення аномалій.

Основні функції Stealthwatch:

- Глибока видимість по периметру мережі, ЦОД та приватна та публічна хмари
- Спрощене розуміння нормальної поведінки мережі за допомогою NetFlow
- Безперервний моніторинг пристроїв, програм та користувачів у розподілених мережах
- Глибокі можливості розслідування інцидентів та аналіз контекстної загрози з докладними ланцюжками аудиту даних NetFlow
- Легка інтеграція з наявною мережевою інфраструктурою (включаючи пристрої без телеметрії Cisco), аналізатором безпеки Cisco, міжмережевими екранами Cisco ASA, Cisco ISE, рішеннями, що підтримуються технологією Cisco TrustSec, та безліччю інших рішень для безпеки.

Stealthwatch Cloud

Stealthwatch Cloud — це рішення, що надається SaaS на базі мережі Інтернет, яке забезпечує наскрізну видимість, аналіз поведінки та виявлення загроз у вашій приватній мережі, загальнодоступній хмарі та гібридних середовищах. Stealthwatch Cloud надає якісні повідомлення про зміни в поведінці, які спостерігаються у вашій

мережі, не витрачаючи дорогоцінний час на IT-фахівців та співробітників служби безпеки. Будучи веб-платформою, Cisco Stealthwatch Cloud є незалежною від платформи і може працювати в будь-якому хмарному середовищі, включаючи Amazon Web Services (AWS) та Microsoft Azure. Stealthwatch Cloud також може здійснювати моніторинг невеликих та середніх приватних мереж та гібридних інфраструктур, що об'єднують локальні та хмарні розгортання. Stealthwatch Cloud може експортувати інформацію про загрози та поведінку до ряду служб безпеки та веб-сервісів, включаючи Cisco Spark, Datadog, Hipchat, PagerDuty, Slack та SIEM та підтримує стандартні формати, такі як електронна пошта та syslog.

Моніторинг громадської хмари

Stealthwatch Cloud забезпечує можливості видимості та виявлення загроз, необхідні для забезпечення високої безпеки ваших робочих навантажень в інфраструктурах AWS та Microsoft Azure. Це хмарне рішення SaaS, яке можна легко та швидко розгортати. В рамках AWS Stealthwatch Cloud AWC VPC Flowlogs моделює поведінку кожного хмарного ресурсу – метод, який називають сутнісним моделюванням. Потім він здатний виявляти раптові зміни у поведінці, зловмисній діяльності та ознаках компрометування. VPC Flowlogs доступні без розгортання програмного забезпечення для ресурсів AWS, а просто для зміни конфігурації у вашій консолі AWS.

Моніторинг приватної хмари

Приватний мережевий моніторинг Stealthwatch Cloud може забезпечити видимість, необхідну для виявлення загроз у мережі в режимі реального часу, без потреби дорогого обладнання, IT-ресурсів або часу служби безпеки.

Моніторинг приватної мережі Cisco Stealthwatch Cloud забезпечує видимість та виявлення загроз для локальної мережі, що постачається з хмарного рішення SaaS. Це кращий вибір для організацій, які хочуть підвищити обізнаність та безпеку у своїх приміщеннях, одночасно скорочуючи капітальні витрати та накладні витрати.

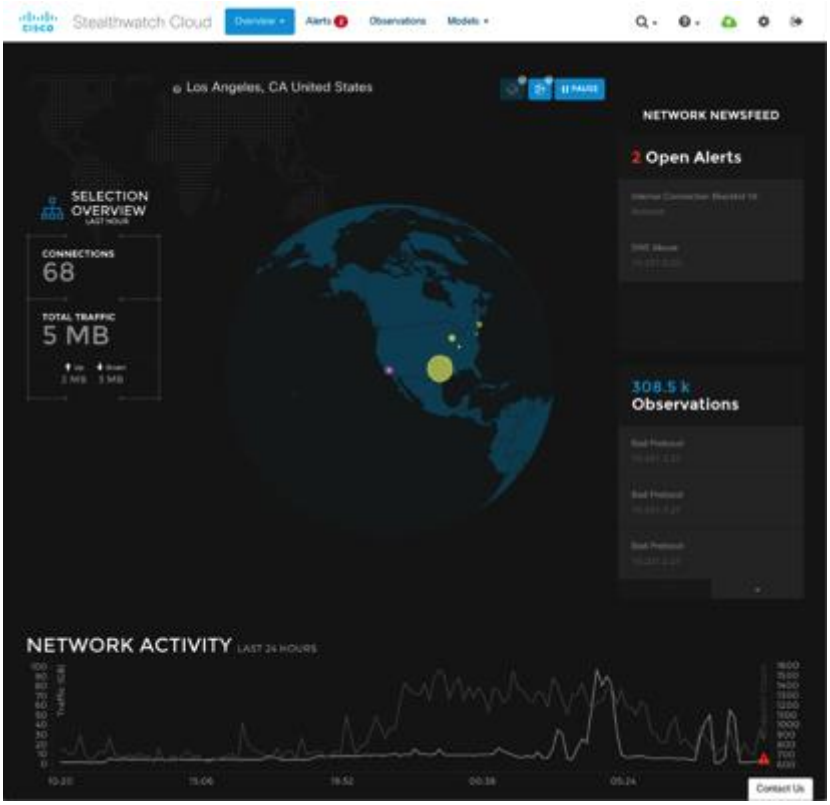

Рис. 3.1. Інтерфейс Cisco Stealthwatch Cloud

Компоненти Cisco Stealthwatch Cloud:

- Моніторинг публічної хмари

Інформація збирається з публічних хмарних сервісів, таких як Amazon Web Services, для створення моделей використання даних у цих хмарах. Потім моделювання хмарних ресурсів застосовується спостереження за раптовими змінами у поведінці, зловмисної діяльності тощо. особливості:

Рішення SaaS, що поставляється з хмари для швидкого та простого розгортання

Виявлення загроз у публічних хмарах

Інтеграція інтерфейсу користувача для Amazon Inspector

- Моніторинг приватної хмари

Моніторинг приватної хмари може забезпечити видимість, необхідну для виявлення загроз у мережі в режимі реального часу, без необхідності дорогого обладнання, IT-ресурсів або часу працівників служби безпеки. особливості:

Широкий спектр мережевої телеметрії та журналів

Інтеграція з фізичними мережами та приватними віртуальними середовищами, такими як гіпервізори VMware

Використовується той самий портал, що й моніторинг публічної хмари

Cisco Stealthwatch Enterprise

Пакет Cisco Stealthwatch Enterprise включає такі рішення безпеки:

Cisco Stealthwatch Management Console: забезпечує єдину точку зору розрізнених IT-груп, щоб побачити поведінкову інформацію про трафік в мережі. Простий інтерфейс дозволяє операторам швидко виявляти проблеми та відповідно реагувати на них.

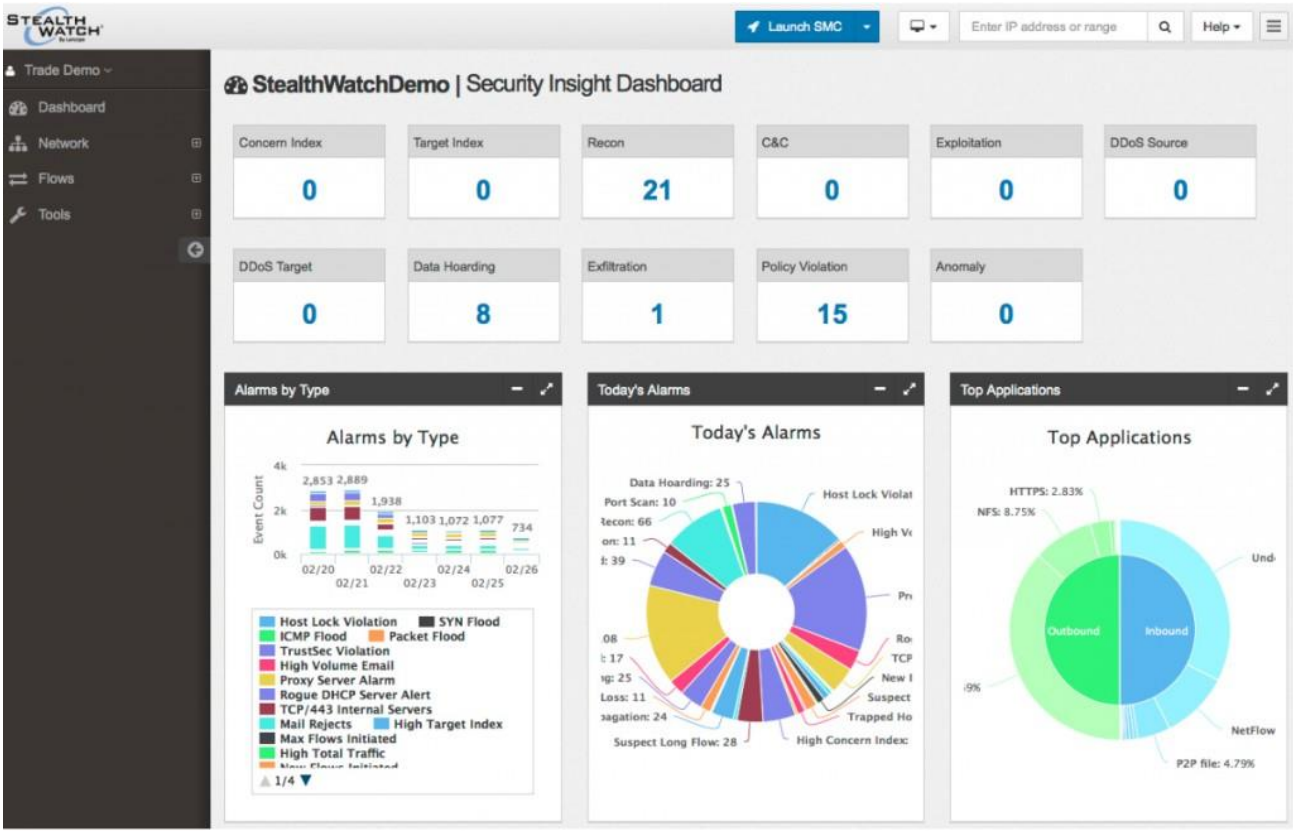

Рис. 3.2. Виявлення інформації про трафік в мережі

Консоль управління Stealthwatch забезпечує такі основні функції:

Відстеження користувачів

Гнучкі можливості розгортання, включаючи віртуальні пристрої

Швидкий аналіз основної причини та усунення несправностей

Реляційні карти потоків

Зшивання NAT

Настроювані інструментальні панелі (dashboard)

Звіти, що настроюються

Автоматизоване блокування, усунення проблем та обмеження швидкості

Звіти типу Top-N для додатків, сервісів, портів, протоколів, вузлів, однорангових вузлів та сеансів

Розбивка трафіку на складові

Настроюваний інтерфейс користувача на базі технології Point-of-View™

Підтримка багатогігабітних мережевих середовищ та великомасштабних мережевих середовищ з багатопротокольною комутацією на основі міток (MPLS)

Розширена візуалізація потоку

Масова масштабованість

Комбінований внутрішній та зовнішній моніторинг

Планування пропускної спроможності та визначення тенденцій на базі історичних даних про трафік

Звітність про оптимізацію WAN

Використання смуги пропускання за допомогою точки коду диференційованих послуг (DSCP)

Візуалізація поширення хробаків

Внутрішній захист для високошвидкісних мереж

Cisco Stealthwatch Flow Collector: дозволяє покращити видимість мережі та безпеку у фізичних та віртуальних середовищах для покращення реагування на інциденти.

Cisco Stealthwatch Flow Sensor: генерує дані NetFlow для сегментів інфраструктури комутації та маршрутизації, які не підтримують NetFlow. Він також

забезпечує повну оглядовість показників продуктивності мережі та сервера. Результатом є оптимізована безпека, мережеві операції та продуктивність додатків.

Компоненти Cisco Stealthwatch Enterprise:

Cisco Stealthwatch Management Console

Консоль керує та налаштовує пристрої Stealthwatch, розгорнуті у різних сегментах вашого підприємства. Консоль управління також може збирати дані з інших технологій, включаючи брандмауери, веб-проксі, системи управління доступом до мережі (NAC) та багато іншого. Різноманітні IT-команди можуть легко отримувати повсюдну видимість мережі та ефективні засоби безпеки для виявлення та визначення пріоритетів загроз безпеці за допомогою єдиної точки зору. Консоль доступна як апаратний пристрій або віртуальна машина.

особливості:

Поглиблена видимість та контекст, заснований на поведінці, захищають від APT, шкідливих програм, інсайдерських загроз, хробаків, вірусів, цілеспрямованих атак, DDoS-атак. Розширені можливості виявлення зменшують час між початком та вирішенням загрози

Телеметрія в реальному часі забезпечує потік даних для одночасного моніторингу трафіку через сотні сегментів мережі для виявлення підозрілої поведінки мережі

Надійна мережева телеметрія полегшує моніторинг продуктивності, планування пропускної спроможності та покращує управління мережею. Це також скорочує трудомісткий та ресурсомісткий ручний аналіз

Групи мережевих пристроїв, графічні уявлення та карти взаємозв'язків забезпечують простий перегляд трафіку вашої організації протягом кількох секунд, показуючи, на що необхідно звернути увагу

Кілька категорій аварійних сигналів та оповіщення на основі контексту домашньої панелі моніторингу дозволяють швидко оцінити положення вашої

організації в безпеці. Це дозволяє вживати рішучих заходів для пом'якшення потенційної шкоди

Функціональність, що масштабується, добре працює у високошвидкісних середовищах і може захистити кожну частину мережі, доступну через IP, незалежно від розміру

Cisco Stealthwatch Flow Collector

Flow Collector збирає та аналізує величезні обсяги мережевих даних з ваших пристроїв. Результатом цього є огляд видимості та безпеки у фізичному та віртуальному середовищі, що покращує реакцію на інцидент. Flow Collector забезпечує економічно ефективну поведінкову аналітику та розширений контекст безпеки. Це дозволяє виявити раннє виявлення аномалій, швидке визначення причин та підвищити захист для широкого спектру загроз, включаючи APT, інсайдерські загрози, DDoS та шкідливе програмне забезпечення Zero-day. Рішення доступне як апаратний або віртуальний пристрій.

Особливості:

Виявлення аномалій на основі потоку вказує на незвичайну поведінку та негайно відправляє сигнал тривоги, сприяючи швидкому та рішучому реагуванню

Дубльовані потоки 1: 1 спрощують моніторинг мережі та безпеки. На додаток до виявлення аномалій в реальному часі, рішення може зберігати дані протягом декількох років, створюючи повний контрольний журнал для поліпшення розслідувань

Простота оновлення дозволяє почати з малого та розширюватися в міру зміни вашої ємності. При повному навантаженні Flow Collector може обробляти дані із 50 000 джерел потоку до 6 мільйонів потоків за секунду (fps)

Cisco Stealthwatch Flow Sensor (опціонально)

Цей компонент забезпечує надійну видимість показників продуктивності мережі, додатків та серверів. Забезпечує економічний метод усунення несправностей безпеки та проблем із продуктивністю програм, а також усуває небезпечні мережеві

сліпі точки. Він може надавати інформацію про програму рівня 7 для середовищ, де Cisco Network-Application Application Recognition (NBAR) вимкнено. Рішення доступне як апаратний або віртуальний пристрій для моніторингу середовища віртуальних машин.

Особливості:

Попередження про аномалії в мережі вказують на незвичайну поведінку і негайно надсилають сигнали тривоги, що дозволяє швидко діяти та зменшувати збитки

Дані URL-адреси дозволяють адміністраторам точно визначати, до яких веб-сайтів підключаються користувачі та пристрої, включаючи шлях до файлу. Це покращує ідентифікацію програм, що викликають проблеми з продуктивністю або безпекою

Підвищена операційна ефективність знижує витрати за рахунок виявлення та ізоляції основної причини проблеми або інциденту протягом кількох секунд

UDP Director (опціонально)

UDP Director спрощує збір та розповсюдження даних про мережу та безпеку на підприємстві. Це допомагає знизити обчислювальну потужність на мережних маршрутизаторах і комутаторах, отримуючи важливу інформацію про мережу та безпеку з кількох місць, а потім пересилаючи її в один потік даних в один або кілька пунктів призначення.

особливості:

Зменшує незаплановані простої та збої в роботі пристрою високої доступності UDP Director 2200

Спрощує мережеву безпеку та моніторинг, надаючи єдиний стандартний пункт призначення для даних NetFlow, SFlow, syslog та SNMP

Надсилає дані UDP з будь-якого UDP-додатка в один або кілька пунктів призначення, за необхідності дублюючи дані

Додаткові ліцензії Cisco Stealthwatch Enterprise

Cisco Stealthwatch Enterprise також має додаткові ліцензії для підвищення продуктивності при взаємодії з іншими продуктами Cisco Security.

Flow Rate License: потрібний для збору, управління та аналізу потоків телеметрії та агрегації потоку в консолі управління. Flow Rate License також визначає обсяг потоків, які можуть бути зібрані та ліцензовані на основі потоків за секунду (fps). Ліцензії можуть бути поєднані для досягнення бажаного рівня пропускної спроможності.

Cisco Stealthwatch Proxy License: забезпечує додаткові можливості для виявлення аномалій з проксі-серверів на консоль управління. Ця ліцензія дозволяє порівняти інформацію, надіслану з проксі-серверів, та надає інформацію про перехоплення веб-трафіку проксі-сервером, що забезпечує більш глибоку видимість веб-трафіку.

Cisco Stealthwatch Threat Intelligence License: корелює дані потоку, щоб забезпечити розширені можливості виявлення APT, включаючи активність ботнетів. Функціональність виявлення ботнетів включає докладний звіт про трафік і аналіз повідомлень команд і управління.

Cisco Stealthwatch Learning Network License: ідентифікує трафік на рівні мережевих пристроїв, використовуючи розпізнавання програм на основі мережі, локалізовані дані мережевого потоку та датчики машинного навчання. Це програмне забезпечення знаходиться на маршрутизаторах серії ISR 4000. Це допоможе вам прийняти обґрунтовані рішення за міткою або відкиданням підозрілих пакетів, що дозволяє прискорити реакцію інцидентів і знизити рівень завантаження пристрою.

Cisco Stealthwatch Endpoint License: дозволяє збирати дані програм, інтегруючи їх із Cisco AnyConnect® Secure Mobility Client. Cisco Stealthwatch Endpoint License отримує дані від клієнта Cisco AnyConnect Secure Mobility і передає ці дані Stealthwatch для аналізу та звітності в консолі управління Stealthwatch.

3.3. Порівняльний аналіз рішень Cisco Stealthwatch і ExtraHop Reveal(x)

ExtraHop Reveal(x) і Cisco Stealthwatch використовують мережу як джерело даних для виявлення та розслідування інцидентів безпеки, але є ключові відмінності в двох продуктах, які важливо розуміти. Однією з ключових відмінностей є те, що Stealthwatch покладається на дані NetFlow, які є лише вибіркою мережевих даних і не надають видимості корисного навантаження транзакцій додатків.

Reveal(x) аналізує мережеві та прикладні протоколи, щоб забезпечити глибшу видимість, що надає кращі можливості виявлення та дослідження, які неможливі з рішенням лише Netflow, таким як Stealthwatch.

Видимість мережі

Що бачить Reveal(x): трафік L2-L7 з безперервним PCAP і розшифруванням

Корінь різниці між Reveal(x) і Stealthwatch — джерело даних. Reveal(x) використовує дротові дані в режимі реального часу, отримані з мережі та проаналізовані зі швидкістю лінії до 100 Гбіт/с, щоб отримати понад 4700 показників. Reveal(x) пасивно аналізує трафік, виконує повторну збірку повного потоку, а також аналізує понад 50 корпоративних протоколів, щоб забезпечити повну видимість L2-L7 та аналіз вмісту, навіть якщо дані зашифровані. У межах трафіку Reveal(x) автоматично виявляє та класифікує кожен пристрій у мережі. Цей безперервний аналіз забезпечує завжди точний інвентаризацію активних пристроїв, може ідентифікувати шахрайські та некеровані сутності та підтримує автоматичну класифікацію критичних активів і конфіденційних баз даних.

Видимість фактичного вмісту корисного навантаження транзакції на L7 для кожної окремої транзакції часто є тим, що робить різницю між простою підозрою про атаку та наявністю конкретних, доступних доказів її. Ця різниця в багатстві даних дає Reveal(x) головну перевагу в ефективності машинного навчання, доступності можливостей швидкого судово-медичного розслідування та рівню впевненості аналітиків до автоматизації процесів реагування на захист та відновлення.

Що бачить Stealthwatch: L2-L4 NetFlow і телеметрія

Stealthwatch покладається на L2-L4 NetFlow і дані телеметрії, які надаються маршрутизаторами, комутаторами та датчиками потоку по всій мережі. Це не є поганим за своєю суттю. Продукт може виявити або зробити висновок, які програми чи протоколи використовуються, переглядаючи початкові пакети даних і метадані про потоки. Цей високорівневий перегляд повідомляє, які пристрої розмовляють і скільки, і чи є нормальним для даного пристрою використання певної програми.

Однак відсутність видимості вмісту транзакцій рівня 7 означає, що критична інформація для виявлення та розслідування атак просто недоступна Stealthwatch. Наприклад, коли зловмисники взаємодіють з критично важливими активами, такими як сервери аутентифікації, бази даних або кластери зберігання, для підвищення своїх привілеїв або вилучення даних, вони можуть не створювати аномальні обсяги або шаблони трафіку. Багато зловмисників активно працюють, щоб приховати сліди від цих способів виявлення. Оскільки Stealthwatch не має доступу до корисного навантаження L7 в транзакції, він не може надати повний контекст і, ймовірно, упустить важливі докази для встановлення впевненості атаки, прихованої від очей через відсутність реєстрації та шифрування. Stealthwatch може повідомити вам, що хтось отримав доступ до бази даних, і, можливо, скільки даних було переміщено, але не відомо, які дані були доступні та вилучені. Використовуючи провідні дані, Reveal(x) може забезпечити більший рівень деталізації.

Виявлення відомих і невідомих загроз

Як Reveal(x) виявляє атаки: прогнозне машинне навчання та аналіз загроз

Reveal(x) ідентифікує ризиковані та шкідливі дії за допомогою низки методів, що працюють з багатими даними L2-L7 та понад 4700 автоматично витягнутих функцій. Ці вхідні дані дозволяють Reveal(x) досягти високого ступеня точності та надати аналітикам багаті криміналістичні деталі, включаючи повні розшифровані пакети, одразу після виявлення. Наприклад, система машинного навчання в Reveal(x) дізнається, як виглядає нормальна поведінка в корпоративній мережі кожного клієнта,

і постійно розробляє уточнювані прогнози щодо майбутньої поведінки кожного пристрою. Reveal(x) також дізнається, що таке нормальна поведінка

серед груп однолітків виглядає так. Якщо один DNS-сервер починає працювати інакше, ніж інші, Reveal(x) це помітить. Коли пристрій веде себе інакше, ніж передбачено, і демонструє активність, що відповідає небезпечним подіям або загрозам, Reveal(x) виявляє це і співвідносить зміну поведінки з одним або кількома кроками ланцюга атаки, наведених нижче.

Завдяки багатим даним, зібраним Reveal(x), і прогнозному поведінковому аналізу, який застосовує система машинного навчання, продукт здатний виявляти ніколи раніше невидимі загрози, таємно

низькі та повільні атаки та нові підходи до атак, які залишаться невидимими для платформ, які покладаються на дані нижчої точності та крихкі системи виявлення на основі сигнатур.

На додаток до виявлення машинного навчання, Reveal(x) ідентифікує неправильну поведінку та дії, які перевищують порогові значення, відповідають шаблонам, що викликають відомі проблеми, або відповідають індивідуальним правилам, визначеним вашою командою. Ці виявлення часто покладаються саме на вміст транзакції рівня 7, який забезпечує такі впевнені та переконливі докази зловмисних дій. Такий діапазон і гнучкість виявлення дають змогу групам безпеки розширити свої можливості за межі реактивного виявлення загроз до проактивного моніторингу, полювання та гігієни. Цей підхід є найкращим способом надійно виявити поведінку атаки на ранній стадії, неправильні конфігурації та проблеми з відповідністю.

Reveal(x) також може отримувати дані аналізу загроз із багатьох сторонніх джерел і співвідносити ці дані з показниками та аналізом на основі машинного навчання для швидкого й автоматичного виявлення та контекстуалізації загроз. Можливість інтегрувати розвідку загроз є стандартною функцією Reveal(x) і може

використовуватися для інтеграції будь-якої платної або безкоштовної розвідки загроз у форматі STIX у платформу.

Як Stealthwatch виявляє атаки: відомі зловмисні програми та порушення користувацьких правил

Основним способом виявлення атак Stealthwatch є порівняння спостережуваної поведінки в мережі з "відомо поганою" поведінкою, наприклад порушеннями користувацьких правил, які вручну виявлено клієнтом, або поведінкою, що відповідає відомим шкідливим програмним забезпеченням. Це, по суті, підхід, орієнтований на правила. Навіть при дуже ефективному машинному навчанні ефективність Stealthwatch обмежена через обмеження NetFlow як джерела даних.

Можливості виявлення загроз Stealthwatch покладаються на NetFlow, телеметрію кінцевих точок, механізми політики та доступу, а іноді аналізують початкові пакети даних, але не повний вміст транзакції. Це має серйозні негативні наслідки для якості виявлення Stealthwatch. Якість введення даних для систем машинного навчання безпосередньо впливає на точність виводу. Точки даних, які Stealthwatch витягує з NetFlow і телеметрії, просто недостатньо багаті, щоб система машинного навчання могла використовувати її для отримання надійних результатів, а це означає, що кількість ручного розслідування, необхідного для перевірки виявленої «загрози», імовірно, буде високою.

Для клієнтів Stealthwatch, які купують ліцензію на розвідку загроз для кожного зі своїх Stealthwatch Flow Collector, продукт також може використовувати дані аналізу загроз Cisco, щоб спрацювати тривогу, повідомляючи аналітикам, чи зв’язуються з їхньою мережею відомі погані IP-адреси або домени.

Що робити, якщо дані зашифровані?

Оскільки підприємства рухаються до шифрування все більшого і більшого трафіку, як внутрішнього, так і зовнішнього зв’язку, процес аналізу даних для виявлення загроз і

розслідування стає все більш складним. Зловмисники це знають і все частіше маскують свою поведінку в існуючому зашифрованому трафікі, як у точках входу/виходу, так і у внутрішньому коридорі схід-захід.

Як Reveal(x) працює із зашифрованими даними: дешифрування поза діапазоном для аналізу

Reveal(x) здатний розшифровувати та аналізувати трафік зі швидкістю рядка, не завдаючи шкоди безпеці та продуктивності. Ця можливість дає вам глибоку видимість, необхідну для швидкого виявлення загроз, розслідування інцидентів і реагування на них. Рішення працює, навіть якщо ввімкнено ідеальну пряму конфіденційність з ефемерними ключами сеансу, що означає, що підприємства можуть підтримувати повну видимість аналізу, яка їм потрібна, водночас користуючись перевагами безпеки та конфіденційності останньої та найкращої версії TLS. Нещодавні дослідження EMA щодо шифрування засвідчили, що 76% респондентів заявили, що планують запровадити TLS 1.3 та ідеальну пряму секретність. Якщо команда безпеки не зможе розшифрувати для аналізу, цей крок не дозволить їм виявити або розслідувати багато атак. Розшифровка даних для виявлення загроз швидко стає необхідною практикою для груп безпеки.

Як Stealthwatch працює із зашифрованими даними: обмежений аналіз зашифрованих пакетів

Stealthwatch не може розшифрувати дані для аналізу, але вони стверджують, що можуть виявляти загрози, проводячи аналіз зашифрованого трафіку. Щоб обійти це обмеження, Cisco використовує оновлену форму NetFlow, яка доступна лише для пристроїв Cisco останнього покоління, для підживлення аналізу зашифрованого трафіку. Ця нова версія NetFlow включає деякі фрагменти даних, витягнуті з початкового пакету даних з кожного потоку, а також послідовність довжини і часу пакетів (SPLT), яка, як стверджує Cisco, «пропонує важливі ключі до вмісту трафіку після початку зашифрованого потоку. " По суті, вони кажуть, що вміст всередині

зашифрованого трафіку дуже корисний, але вони не можуть його побачити, тому висновки на основі зовнішніх підказок є найкращим, що у них є.

Давайте розберемося, що означають ці нові точки даних.

● Початковий пакет даних — це крихітна частина розмови, яка доступна для аналізу до того, як решта транзакції стане зашифрованою. З цього Stealthwatch може отримати деякі відомості про рівень застосованого шифрування, а також HTTP-URL-адреси та імена хостів DNS.

● Послідовність довжини і часу пакетів (SPLT) по суті є грубою ознакою поведінки. Stealthwatch вимірює розмір пакетів і час між їх надходженням і порівнює це з моделями передачі даних, пов’язаними з відомими сімействами шкідливих програм.

Це означає, що вони дивляться, хто з ким розмовляє, і роблять деякі обчислення щодо розподілу байтів і часу пакетів, щоб зробити напівобґрунтоване припущення про те, що може міститися в комунікаціях. Вони можуть отримати деяку інформацію про пакет HTTPS, але не можуть підтвердити, що було насправді надіслано або запитано, або чи містить запит HTTP шкідливий код, як у випадку міжсайтових сценаріїв або атак із застосуванням SQL. Це означає, що Stealthwatch не може впевнено виявити багато типів атак, які покладаються на навмисне зловживання корисним навантаженням зашифрованої транзакції, включаючи атаки міжсайтових сценаріїв, ін’єкції SQL та маніпуляції з базою даних, як-от видалення таблиці аудиту. Вони можуть помітити незвичайні рівні комунікації між хостами, але їм доведеться повідомити аналітиків, щоб вони далі досліджували, використовуючи інші інструменти, такі як журнали, щоб переконатися, що те, що сталося, було атакою, а не просто незвичайною поведінкою. Оскільки журнали часто не вмикаються на серверах баз даних і DNS, які є основними векторами та об’єктами атак, подальше дослідження може бути неможливим.

Крім того, зловмисники регулярно модифікують свої методи, щоб уникнути виявлення на основі правил, тому грубі дані ще рідше дадуть необхідний сигнал для впевненого виявлення. Це призводить до великої кількості помилкових спрацьовувань, витрачання часу та енергії аналітика і, зрештою, до пропуску сигналів фактичних атак.

Reveal(x) може бачити вміст 7-го рівня транзакцій у цих атаках, а це означає, що аналітики можуть відразу побачити, чи завантажив користувач обмежені дані чи видалив журнали. Вони можуть впевнено перейти до виправлення, замість того, щоб витрачати час на перехід до інших інструментів, щоб перевірити, чи виправдовує попередження Stealthwatch розслідування.

Робочі процеси дослідження та відновлення

Як працюють розслідування та відновлення в Reveal(x)

Reveal(x) зосереджується на забезпеченні швидких, переважно автоматизованих робочих процесів розслідування, щоб аналітики мали всю необхідну інформацію, щоб впевнено реагувати, як тільки вони отримають виявлення. Кожне виявлення надається з багатим контекстним уявленням, пропонуючи аналітику чіткий шлях для дослідження, а також прямі посилання на дані та зв’язки, які слід досліджувати. Протягом одного кліка після отримання виявлення, аналітики, які використовують Reveal(x), можуть отримати доступ до повністю індексованих записів транзакцій із можливістю пошуку та повного вмісту пакетів для всіх пристроїв, транзакцій і користувачів, залучених до потенційної загрози. Це дає змогу аналітикам швидко й впевнено реагувати на загрозу найбільш підходящим способом, без необхідності переходити між інструментами та вручну переглядати величезні файли PCAP, щоб точно з’ясувати, що сталося. Аналітики рівня 1 можуть досягти більше з меншим навчанням і наглядом, і кожен аналітик працює в більш продуктивному середовищі.

У Reveal(x) дослідження виявлення можна почати з будь-якої точки інтерфейсу. Анотації виявлення з’являються на картах активності в реальному часі, списках пристроїв, діаграмах активності та на сторінці огляду безпеки, тому аналітики можуть

швидко побачити, де відбулися виявлення, і зрозуміти їх контекст. Одним клацанням миші аналітики можуть побачити всі виявлення, пов’язані з певним хостом, включаючи оцінку ризику, що вказує на відносну серйозність проблеми, зв’язок із розвідкою загроз третьої сторони, імена користувачів, пов’язані з виявленням, довідкову інформацію про тип атаки, кроки для пом’якшення, і рекомендував наступні кроки для розслідування.

Типовий робочий процес для розслідування загроз у Stealthwatch включатиме перегляд списку IP-адрес, з якими пов’язані події безпеки, вибір однієї для дослідження та перегляд списку подій безпеки, пов’язаних з цим хостом, щоб вирішити, продовжувати чи ні. санація. Для багатьох подій безпеки цей процес розслідування, імовірно, вимагатиме повороту, щоб вручну запитувати інші системи, такі як SIEM або інструмент захоплення пакетів, щоб встановити достатню впевненість, щоб гарантувати поміщення в карантин потенційно скомпрометованого хоста або інсайдерської загрози. Це вказує на ще одну проблему зі Stealthwatch: залежності. Продукт значною мірою покладається на інші продукти Cisco, такі як механізм Identity Services Engine (ISE), аналіз загроз Talos, аналізатор пакетів безпеки та інші, щоб виконати свої обіцянки. Stealthwatch сам по собі є лише частковим рішенням і шлюзом до набагато більших витрат на продукти Cisco.

З порівняння можна виявити, що у представлених прикладів дуже багато переваг, тому потрібно вибирати згідно з власних умов, або тих, які виставлені в компанії.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми забезпечення безпеки комп'ютерних мереж. Проаналізовано існуючі технології забезпечення безпеки комп'ютерних мереж інформаційної системи від аномалій. Досліджена технологія забезпечення безпеки комп'ютерних мереж інформаційної системи від аномалій на базі Cisco Stealthwatch.

Встановлено основні функції та принципи роботи програмного комплексу Cisco Stealthwatch. Cisco Stealthwatch може отримувати додаткову контекстну інформацію для визначення та визначення пріоритетності нових і нових загроз у розширеній мережі. Розширена аналітика безпеки дає змогу мати глибокий аналіз як веб-трафіку, так і мережевого трафіку. Ця контекстна інформація забезпечує видимість та аналітику, що дає вам можливість ідентифікувати та визначити пріоритети загроз у розширеній мережі. Тепер ви можете виявляти загрози, які обійшли існуючі засоби контролю безпеки, і виявляти ексфільтрацію даних до легальних хмарних служб

Використання Cisco Stealthwatch надає компанії доступ до широкого набору функцій безпеки в тому числі:

- Глибока видимість по периметру мережі, ЦОД та приватна та публічна хмари
- Спрощене розуміння нормальної поведінки мережі за допомогою NetFlow
- Безперервний моніторинг пристроїв, програм та користувачів у розподілених мережах
- Глибокі можливості розслідування інцидентів та аналіз контекстної загрози з докладними ланцюжками аудиту даних NetFlow
- Легка інтеграція з наявною мережевою інфраструктурою (включаючи пристрої без телеметрії Cisco), аналізатором безпеки Cisco, міжмережевими екранами Cisco ASA, Cisco ISE, рішеннями, що підтримуються технологією Cisco TrustSec, та безліччю інших рішень для безпеки.

У роботі запропоновано варіант технології забезпечення безпеки мережевого трафіку

інформаційної системи від аномалій на базі Cisco Stealthwatch.

Розроблено рекомендації фахівцям із кібербезпеки щодо застосування технології забезпечення безпеки мережевого трафіку інформаційної системи від аномалій на підприємстві.

.

ПЕРЕЛІК ПОСИЛАНЬ

1. Вычислительные машины, сети и телекоммуникационные системы. [Електронний ресурс] – Режим доступу: https://lawbooks.news/sistemyi-telekommunikatsionnyie-kompyuternyie/vyichislitelnyie-mashinyi-seti.html

2. What is Computer Networking? [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/what-is-computer-networking/

3. Основы компьютерных сетей. Тема №1. Основные сетевые термины и сетевые модели [Електронний ресурс] – Режим доступу: https://habr.com/ru/post/307252/

4. Science of Network Anomalies [Електронний ресурс] – Режим доступу: https://www.flowmon.com/en/blog/science-of-network-anomalies#what-is-network-anomaly

5. ExtraHop Reveal(x) vs. Cisco Stealthwatch [Електронний ресурс] – Режим доступу: https://assets.extrahop.com/whitepapers/Technical-Brief-Reveal%28x%29-vs.-StealthWatch.pdf

6. Причины и источники сетевых аномалий [Електронний ресурс] – Режим доступу: https://moluch.ru/archive/102/23376/

7. Разработка системы обнаружения аномалий сетевого трафика [Електронний ресурс] – Режим доступу: https://journals.nstu.ru/vestnik

8. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов. / Под ред. профессора О. И. Шелухина – М.: Горячая линия–Телеком, 2013. – 220 с: ил. ISBN 978-5-9912-0323-4.

9. Информационная безопасность в компьютерных сетях [Електронний ресурс] – Режим доступу: https://lawbooks.news/telekommunikatsionnyie-sistemyi-kompyuternyie/informatsionnaya-bezopasnost-kompyuternyih-60855.html

10. 5 Common Network Security Problems and Solutions [Електронний ресурс] – Режим доступу: https://www.compuquip.com/blog/network-security-problems-solutions

11. Network security issues [Електронний ресурс] – Режим доступу: https://www.nibusinessinfo.co.uk/print/node/10230

12. Системы обнаружения аномалий: новые идеи в защите информации [Електронний ресурс] – Режим доступу: http://citforum.ck.ua/security/articles/anomalis/

13. Описание решения Cisco StealthWatch [Електронний ресурс] – Режим доступу: https://www.compuway.ru/productline/security/siem/cisco-stealthwatch/

14. An Introduction To Cisco Stealthwatch [Електронний ресурс] – Режим доступу: https://tesrex.com/article/an-introduction-to-cisco-stealthwatch/

15. Cisco StealthWatch или классические средства защиты корпоративной сети [Електронний ресурс] – Режим доступу:https://habr.com/ru/company/tssolution/blog/414195/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)