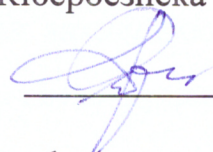


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

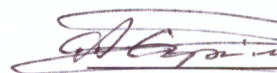
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захисту та аналізу захищеності особистої інформації у мережі»

Виконав студент 2-го курсу групи ЗКБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»

 Сергій Ядчишин

Керівник, завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 Андрій Єфіменко

Рецензент, професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

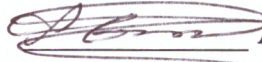
 Володимир Воротніков

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

17 вересня 2024 р.

ЗАВДАННЯ
на випускню кваліфікаційну роботу

Студент: Ядчишин Сергій Іванович

Тема роботи: «Методи та технології захисту та аналізу захищеності особистої інформації у мережі»

Затверджена наказом університету від 17 вересня 2024 р. № 480/с

Термін здачі студентом закінченої роботи 26 грудня 2024 р.

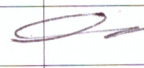
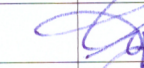
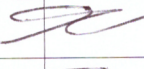
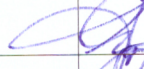
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

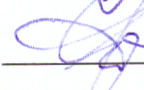
Об'єктом дослідження є пошук та дослідження застосунків та інструментів для захисту та аналізу захищеності персональних даних у мережі. Предметом дослідження є технології та шляхи перевірки захищеності персональних даних використовуючи загальнодоступні застосунки та інструменти.

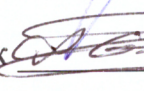
Обладнання та програмне забезпечення:

1. ПК з можливістю віртуалізації
2. Програмне забезпечення віртуалізації: VirtualBox
3. Операційні системи: Windows, Ubuntu, Kali Linux
4. Програмне забезпечення Nmap, Wireshark, MegaPing; Cisco Secure IPS (NGIPS), Amazon Web Services (AWS) GuardDuty, Azure Firewall Premium IDPS, Darktrace Enterprise Immune System

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються:

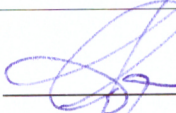
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Юрій Россінський	 17.09.2024	 17.09.2024
2	Юрій Россінський	 17.09.2024	 17.09.2024
3	Юрій Россінський	 17.09.2024	 17.09.2024

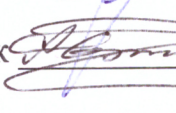
Студент  С.І. Ядчишин

Керівник  А.А. Єфіменко

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	01.03.2024	виконано
2	Розробка плану роботи	02.04.2024	виконано
3	Розробка розгорнутого плану	09.04.2024	виконано
4	Подача чернетки керівнику для перевірки	16.04.2024	виконано
5	Доопрацювання роботи та перевірка керівником	20.06.2024	виконано
6	Затвердження графічних матеріалів у керівника	20.07.2024	виконано
7	Проведення попереднього захисту	19.11.2024	виконано
8	Отримання відгуку керівника	19.11.2024	виконано
9	Допуск завідувача кафедри	01.12.2024	виконано
10	Подання роботи на рецензування	01.12.2024	виконано

Студент  Сергій Ядчишин

Керівник  Андрій Єфіменко

АНОТАЦІЯ

Завдання кваліфікаційної роботи магістра полягає у розкритті проблематики посягання на збереженість персональної інформації (даних) зловмисниками шляхом здійснення кібератак на мережеву інфраструктуру та кінцеві пристрої, вивченні інструментів, програмно-апаратних рішень та методів виявлення загроз витоку персональних даних в мережі.

Розкрито питання застосування загальнодоступних інструментів які виявляють невидимі загрози, що можуть означати кібератаку, та систем виявлення та запобігання вторгненню, рекомендованих Міністерством цифрової трансформації України. Розкрито питання застосування інструментів Kali Linux, Nmap, Wireshark , MegaPing для аналізу рівня захищеності особистої інформації в мережі та на кінцевих пристроях.

Кваліфікаційна робота магістра на тему “Методи та технології захисту та аналізу захищеності особистої інформації у мережі” складається з теоретичного, логічного, інженерного, аналітичного комплексів та пояснювальної записки.

Пояснювальна записка до випускної роботи містить в собі 91 сторінок, матеріали доповнені таблицями, ілюстраціями в кількості 43 та схемами. Список використаних джерел містить 16 джерел.

КЛЮЧОВІ СЛОВА: ПЕРСОНАЛЬНІ ДАНІ, КІБЕРБЕЗПЕКА, ЗАГРОЗА, КОНФІДЕНЦІЙНІСТЬ, ТЕСТУВАННЯ, АУТЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ, МОНІТОРИНГ, РЕАГУВАННЯ.

ANNOTATION

The task of the master's thesis is to reveal the problems of encroachment on the security of personal information (data) by intruders through cyberattacks on network infrastructure and end devices, to study tools, software and hardware solutions and methods for detecting threats of personal data leakage in the network.

The article discusses the use of publicly available tools that detect invisible threats that may indicate a cyberattack and intrusion detection and prevention systems recommended by the Ministry of Digital Transformation of Ukraine. The issues of using Kali Linux, Nmap, Wireshark, MegaPing tools to analyse the level of security of personal information on the network and on end devices are covered.

The master's qualification work on the topic 'Methods and technologies of protection and analysis of personal information security in the network' consists of theoretical, logical, engineering, analytical complexes and an explanatory note.

The explanatory note to the final thesis consists of 91 pages, and the materials are supplemented with tables, screenshots 43 and diagrams.

KEYWORDS: PERSONAL DATA, CYBERSECURITY, THREAT, PRIVACY, TESTING, AUTHENTICATION, ACCESS CONTROL, MONITORING, RESPONSE.

Зміст

<u>ВСТУП</u>	8
<u>РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ РОБОТИ</u>	12
<u>1.1 Обґрунтування актуальності теми методів та технологій захисту та аналізу захищеності особистої інформації в мережі</u>	12
<u>1.2 Захист персональних даних за українським законодавством</u>	13
<u>1.3 Дефініція визначень подія, кіберінцидент, кібератака</u>	14
<u>1.4 Соціальна інженерія як метод нападу на персональні дані</u>	20
<u>1.5 Необхідність розробки системи аналізу захищеності інформації в інформаційно-комунікаційних системах і мережах</u>	27
<u>РОЗДІЛ 2 ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В ІТС</u>	31
<u>2.1 Захист персональних даних від атак за допомогою алгоритмів соціальної інженерії</u>	31
<u>2.2 Антивірусні технології</u>	33
<u>2.3 Технології виявлення та блокування кібератак на кінцевих пристроях</u>	37
<u>2.4 Технології протидії витокам інформації</u>	40
<u>2.5 Технологія обману в захисті ІТС</u>	44
<u>2.6 Технології механізму безпечного виконання програм</u>	45
<u>РОЗДІЛ 3 АНАЛІЗ РІВНЯ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ</u>	48
<u>3.1 Тест на проникнення, застосування інструментів Kali Linux, Nmap, Wireshark , MegaPing</u>	48
<u>3.2 Інструменти що виявляють невидимі загрози, які можуть означати кібератаку, Zscaler Deception, FortiDeceptor, CyberTrap, Cisco Stealthwatch, Illusive Shadow</u>	60
<u>3.3 Системи виявлення та запобігання вторгненню, Cisco Secure IPS (NGIPS), Amazon Web Services (AWS) GuardDuty, Azure Firewall Premium IDPS, Darktrace Enterprise Immune System</u>	72
<u>ВИСНОВКИ</u>	89
<u>СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ</u>	91

ВСТУП

У наш час інтернет остаточно став глобальною – не лише за принципами організації, а й за кількісними показниками – мережею, кількість його користувачів уже наблизилася до трьох мільярдів і продовжує швидко зростати. Нині приблизно третина населення Землі користується інтернетом. Так само швидко вдосконалюються ІТ, їх виробничі потужності, масового розповсюдження набула багатофункціональна й високопродуктивна мобільна електроніка. Уже сьогодні інтернет і асоційовані з ним інформаційні технології, сервіси та комунікативні середовища є дійсно всеохоплюючою, загальнодоступною і абсолютно необхідною для нормальної життєдіяльності людства структурою.

Визнання права людини на анонімність в он-лайні завжди було одним із стовпів архітектури та філософії інтернету. Водночас за логікою цієї ж архітектури без розміщення особою персональних даних на віддалених серверах (а отже, у мережі) повноцінне послуговування всіма її вигодами є неможливим.

Кожного разу, підключаючись до мережі, пристрій користувача автоматично реєструється в ній, вказуючи унікальний ідентифікатор – IP-адресу, телефонний номер комутованого з'єднання, абонентський номер договору з оператором доступу та інші, необхідні для реєстрації в мережі, дані. Далі, мандруючи інтернетом, особа залишає за собою інформаційний «шлейф», що складається з ще більшої кількості відомостей. Нижче наведено мінімальний перелік даних, які автоматично передаються і залишаються в мережі при кожному відвіданні будьякого веб-ресурсу:

- веб-адреса сторінки, що переглядається (URL);
- веб-адреса сторінки, що посилається на першу;
- унікальна IP-адреса, найменування провайдера, країна реєстрації, місцезнаходження пристрою;
- параметри браузера (тип, версія, мова, налаштування, підтримка додатків) та комп'ютера (основні апаратні можливості, операційна система, роздільна здатність екрану тощо);
- дані проксі-сервера;

- дані про підтримку cookies¹⁵ і Java;
- часовий пояс.

В умовах нинішньої тотальної «інтернетизації» інфраструктур – телекомунікацій, систем транспортування, фінансів, обліку населення, медичного обслуговування, численних баз даних багаторазово збільшує кількість та якість інформації, що опрацьовується щодо кожної особи в кіберпросторі, причому часто без її відома. Стрімко розвиваються також публічні онлайн-сектори, де населення масово та усвідомлено залишає свої персональні дані: електронний бізнес, банкінг і шопінг, цілий спектр онлайн-послуг, електронна пошта, середо вище Web 2.0.¹⁶ хмарові сервіси, онлайн-аутсорсинг і багато іншого. Ідеться про заповнення відвідувачами різноманітних анкет, реєстрацію та отримання логіна і пароля, реєстрацію з використанням облікового запису соціальної мережі, надання електронної адреси відвідувача для зворотного зв'язку тощо.

Можливість надійного захисту своєї анонімності та персональних даних у такому середовищі стає для користувача майже нульовою, навіть якщо він дотримується рекомендованих вимог безпеки. Апаратні можливості ІТ-обладнання вже досить давно дозволяють не видаляти дані, що обертаються у вебi, і автоматично зберігати їх. Тому незалежно від обраного особою режиму доступу до ПД всі приватні відомості, що розміщуються нею в он-лайнi, або з певних причин потрапляють до мережі з її локальних сховищ, зберігаються у віддалених сховищах і базах даних інтернету. Таким чином, вони залишаються відкритими для несанкціонованого доступу, причому пересічний користувач суб'єкт цих персональних даних зазвичай не має технологічної можливості проконтролювати їх подальшу міграцію та оброблення. Тому з технічного погляду не є особливою проблемою створення детального дос'є на будь-яку особу та/або систематичний збір інформації про неї. Уже не перший рік такі маніпуляції здійснюються та аналізуються комп'ютерними системами в автоматичному режимі. Для зацікавленої людини чи організації питання полягає лише в доступі (законному чи ні) до потрібних інформаційних ресурсів. При цьому можуть оброблятися персональні дані дуже широкого діапазону: від анкетних даних (відомості про

ідентифіковану особу) до відомостей, які можуть стосуватися особи опосередковано або які можуть використовуватися у процесі ідентифікації особи (інформація про оплату послуг з використанням платіжних карт, логіни та паролі, записи в соціальній мережі, номери телефонів, електронні адреси тощо).

У цьому контексті досить закономірними є пов'язані з несанкціонованим витоком персональних даних численні скандали і судові конфлікти між провідними соціальними мережами (Facebook, Twitter, Google+ та інші) з глобальним охопленням і обмежені окремими країнами, з пересічними фізичними чи юридичними особами. Причому нерідко йдеться про незаконний «злам» сотень тисяч аккаунтів. Кількість подібних інцидентів є занадто великою, а самі вони надто стереотипними для того, щоб наводити про них докладну інформацію.

Завершуючи цей огляд основних загроз недоторканності приватного життя людини в кіберпросторі, доречно хоча б коротко згадати про ще одну небезпеку, яка поки що не є цілком очевидною, проте може стати актуальною у найближчому майбутньому. В умовах швидко прогресуючої «інтернетизації» технічних засобів та інфраструктур (насамперед побутових) дедалі важливішим джерелом пов'язаної з особою інформації стають віртуальні пошукові машини, що працюють з т.зв. тіньовим інтернетом – веб-адресами серверів, веб-камер, принтерів, роутерів та іншої підключеної до мережі ІТ-периферії, а також світлофорів, камер безпеки, домашніх систем автоматизації та опалення. Усі ці відомості також можуть групуватися навколо «віртуального образу особи», у контексті інших даних надаючи додаткові подробиці про її приватне життя.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ РОБОТИ

1.1 Обґрунтування актуальності теми методів та технологій захисту та аналізу захищеності особистої інформації в мережі

Актуальність задачі захисту інформації в комп'ютерних системах на сьогоднішній день невіддільна від загального розповсюдження цих систем та поширення комп'ютерних мереж, які обмінюють великі обсяги інформації. Забезпечення безпечної діяльності комп'ютерних систем стало критично важливим для різноманітних підприємств та установ, від державних організацій до невеликих приватних фірм. Незалежно від сфери діяльності, забезпечення конфіденційності та цілісності інформації вимагає розробки та впровадження ефективних методів та засобів безпеки, з урахуванням різноманітних викликів та потреб різних типів організацій. Розходження в цьому питанні полягає в застосуванні різних засобів та методів, а також в обсязі заходів, призначених для забезпечення найвищого рівня безпеки в конкретних умовах використання комп'ютерних систем.

У сучасному цифровому світі, де обсяг інформації, яка зберігається та обробляється в кіберпросторі, непинно зростає, питання захисту персональних даних набуває все більшої актуальності. Персональні дані, такі як фінансова інформація, медичні записи, а також дані соціальних мереж, є цінним ресурсом, який може бути використаний як в легітимних цілях, так і для зловмисних дій. Незважаючи на постійне вдосконалення технологій безпеки, зростаюча складність кіберзагроз та еволюція методів кібератак створюють нові виклики для захисту персональної інформації. У зв'язку з цим виникає необхідність аналізу сучасних проблем захисту персональних даних, зокрема правових, технічних та етичних аспектів цього питання. Забезпечення безпеки персональних даних залишається актуальною проблемою сьогодні, адже дедалі більше людей користуються. Мережею Інтернет, проходять авторизацію на різних ресурсах, використовуючи для цього свої персональні дані, а також дедалі більше різних установ створюють своєрідні бази даних, не завжди дбаючи про їх схоронність. Недостатня міра забезпечення безпеки персональних даних у кіберпросторі призводить до

надмірної активності кібератак та вчинення різних махінацій із персональними даними. Актуальність теми захисту персональних даних в кіберпросторі обумовлена кількома важливими факторами, які мають значний вплив на сучасне суспільство, економіку та безпеку. Основні аспекти, що підкреслюють актуальність цього питання: зростання цифровізації; кіберзагрози; законодавчі вимоги; соціальна відповідальність і довіра; економічні наслідки; технологічні виклики; міжнародні відносини та геополітика. Таким чином, актуальність теми захисту персональних даних в кіберпросторі зумовлена складністю та глобальним характером цього питання, а також його важливістю для збереження приватності, безпеки та довіри в цифровому світі.

1.2 Захист персональних даних за українським законодавством

Закон України “Про інформацію” окреслює конфіденційну інформацію як інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

У сучасному світі найуразливішою ланкою серед усіх кібератак залишається людина. Персональні дані можуть бути як конфіденційною інформацією, так і відкритою. Пункт 2 статті 11 Закону України “Про інформацію” встановлює, що конфіденційними є зокрема дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, місце проживання і/або реєстрації, дата і місце народження.

Закон України “Про захист персональних даних” визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Це найуживаніше визначення даного поняття - і воно є найбільш узагальненим. Перелік відомостей, які належать до персональних даних, змінюється від однієї держави до іншої. Наприклад, інформація про IP-адресу в країнах Європейського Союзу належить до персональних даних, а у Сполучених Штатах Америки ні, проте відноситься до інформації, що пов’язана з персональними даними.

1.3 Дефініція визначень подія, кіберінцидент, кібератака

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кіберпростір - середовище, яке надає можливість для здійснення комунікацій або здійснення реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних. В кіберпросторі наявні потенційно можливі явища і чинники, що створюють небезпеку національним інтересам держави. Основними з них є кіберінциденти та кібератаки. Але кіберінцидент зазвичай характеризується певними відхиленнями в типовій поведінці об'єкта, які називаються аномаліями.

Аномалія - відступ або ухилення від правила, тому аномальним називають все, що відступає або уникає правильного або нормального.

Інцидент кібербезпеки (кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Кіберзагроза (на рисунку порушник) – наявні та потенційно можливі явища і фактори, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Кіберзагроза – фактори (події, явища), які мають місце або можуть виникнути в кіберпросторі, за умови умисного цілеспрямованого або випадкового впливів та створити небезпеку порушення процесів управління і передачі інформації, що відбуваються у кібернетичних системах різних сфер (соціальної, технічної, соціотехнічної), або можуть зашкодити елементам таких систем.

Загроза (threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків

Системна класифікація загроз безпеці інформації		
Параметри класифікації	Значення параметрів	Зміст значення параметрів
Види	Фізична цілісність Логічна структура Зміст Конфіденційність Право власності	Знищення (викривлення) Викривлення структури Несанкціонована модифікація Несанкціоноване отримання Привласнення чужого права
Природа походження	Випадкова Навмисна	Відмови, збої, помилки, стихійні лиха, побічні впливи Злочинні дії людей
Передумова появи	Об'єктивні Суб'єктивні	Кількісна недостатність елементів системи, якісна недостатність елементів системи Розвідувальні органи іноземних держав, промисловий шпіонаж, кримінальні елементи, «недоброяркісні» співробітники
Джерело загроз	Люди Технічні пристрої Моделі, алгоритми, програми Технологічні схеми обробки Зовнішнє середовище	Сторонні особи, користувачі, персонал Реєстрації, передачі, зберігання, видачі Загального призначення, прикладні, допоміжні Ручні, інтерактивні, внутрішньомашинний, мережеві Стан атмосфери, побічні шуми, побічні сигнали

Рисунок 1.1 – Системна класифікація загроз безпеці інформації

Вразливість системи (system vulnerability) — нездатність системи протистояти реалізації певної загрози або сукупності загроз. Вразливості класифікуються відповідно до класу активів, до яких вони відносяться — апаратного забезпечення, програмного забезпечення, комп'ютерної мережі, персоналу, організації, тощо. При виявленні вразливостей їх описують згідно певних вимог баз вразливостей, де вони й зберігаються для подальшого використання аналітиками безпеки. Наразі найбільш поширені наступні бази вразливостей:

- MITRE — Common Vulnerabilities and Exposures (CVE) та Common Weakness Enumeration (CWE) [<http://cve.mitre.org>];
- NIST — National Vulnerabilities Database (NVD) [<http://nvd.nist.gov>];
- United State Computer Emergency Readiness Team — Vulnerability Notes Database (VND) [<http://www.us-cert.gov>];
- IBM — XForce [<http://xforce.iss.net>];
- Open Source Vulnerabilities Data Base — OSVDB [<http://osvdb.org>].

Кібератака – спрямовані дії в кіберпросторі, які здійснюються за допомогою електронних комунікацій та спрямовані на досягнені однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються в технологічних системах, отримання несанкціонованого доступу до таких ресурсів. Тобто різниця понять кіберінцидент й кібератака визначається наявністю мети в дії та спрямованістю в здійсненні. Так кіберінцидент має ймовірнісний характер й не завжди, на противагу кібератаці, має мету здійснення. Кібератака ж виникає з наявної кіберзагрози й спрямована на експлуатацію вразливості в системі захисту або ж в самому об'єкті захисту з метою порушення однієї з властивостей об'єкту захисту. Класифікація кібератак. Атаки на інформаційні системи характеризуються декількома ознаками. Для розгляду їх сутності та умов здійснення пропонується наступна класифікація.



Рисунок 1.2 – Класифікація віддалених атак

За характером впливу віддалені атаки діляться на:

- пасивний вплив;
- активний вплив.

Пасивним впливом на інформаційну систему є вплив, який не має безпосереднього впливу на роботу системи, але може порушувати політику доступу до захищених даних. Саме відсутність впливу на роботу розподіленої системи призводить до того, що пасивний віддалений вплив практично неможливо виявити. Прикладом пасивного типового віддаленого впливу на інформаційну систему служить прослуховування каналу зв'язку в мережі і перехоплення переданої інформації. Активна дія на ресурси системи - це безпосередній вплив на

роботу системи (зміна конфігурації, порушення працездатності і т. д.) і порушує прийняту в ній політику безпеки. Очевидною особливістю активного впливу, в порівнянні з пасивним, є можливість його виявлення (з більшим чи меншим ступенем складності). Прикладом результату такого впливу є відмова в обслуговуванні системи.

За метою реалізації впливу віддалені атаки можуть бути спрямовані на:

- порушення конфіденційності інформації;
- порушення цілісності інформації;
- порушення доступності системи.

Основним результатом практично будь-якого зловмисного впливу на інформаційну систему є отримання несанкціонованого доступу до інформації. Такий доступ досягається шляхом перехоплення або спотворення інформації. Можливість перехоплення інформації означає отримання до неї доступу, але неможливість її зміни (модифікації). Отже, перехоплення інформації веде до порушення її конфіденційності. Прикладом перехоплення інформації є аналіз мережевого трафіку (не слід плутати з санкціонованим проведенням аналізу мережевого трафіку). Спотворення інформації можливо в тому випадку, якщо зловмисник має повний контроль над інформаційним потоком між об'єктами системи і/або має можливість передавати дані під ім'ям довіреного користувача. В цьому випадку, спотворення інформації веде до порушення її цілісності. Даний інформаційний руйнівний вплив відноситься до активного впливу. Прикладом віддаленої атаки, мета якої порушення цілісності інформації, може служити віддалена атака «Помилковий об'єкт мережі».

І зовсім інший вид атаки, коли отримання атакуючим несанкціонованого доступу до інформації не передбачається - це порушення працездатності (доступності) системи. В даному випадку основна мета зловмисника - різке зниження продуктивності системи об'єкта (або виведення її з ладу) на який здійснюється атака, і як наслідок - неможливість доступу користувачів до її ресурсів. Прикладом віддаленої атаки, метою якої є порушення працездатності системи, може служити віддалена атака «Відмова в обслуговуванні» (DoS-атака,

Denial of Service). І найбільш популярний різновид DoS-атаки - DDoS-атака (Distributed Denial of Service), розподілена атака типу «відмова в обслуговуванні»

Для того щоб здійснити віддалений вплив на об'єкт інформаційної системи, необхідне настання певних умов. У розподілених мережах виділяються три умови для початку здійснення впливу:

- атака по запиту. В даному випадку атакуючий чекає від потенційного об'єкта атаки передачі запиту певного типу, який і буде умовою початку здійснення впливу. Прикладом подібних запитів можуть бути DNS і ARP-запити;
- атака по події. Атакуючий веде постійне спостереження за станом операційної системи віддаленої цілі атаки і при виникненні певної події в цій системі починає вплив;
- безумовна атака. В даному випадку початок здійснення атаки безумовно по відношенню до мети атаки, тобто атака здійснюється негайно і незалежно від стану системи чи об'єкта. Атакуючий є ініціатором початку здійснення атаки.

Атаки на ІТС можна класифікувати за наявністю зв'язку з об'єктом. Розрізняють атаки з зворотним зв'язком і без зворотного зв'язку (односпрямована атака). Зворотній зв'язок формується відповіддю об'єкта, який атакується на певний запит, відправлений до нього зловмисником, і дозволяє останньому реагувати на всі зміни, що відбуваються на об'єкті. Метою віддаленої атаки без зворотного зв'язку не є отримання даних від об'єкта атаки. Атакуючий відправляє запити, не чекаючи відповіді від об'єкта. Тому подібну віддалену атаку називають односпрямованою. Як приклад односпрямованої атаки можна привести типову віддалену атаку «Відмова в обслуговуванні».

По розташуванню порушника щодо об'єкта атаки вплив реалізується як всередині сегментна атака, так і між сегментна.

Розглянемо ряд визначень:

- хост (host) - мережевий пристрій (найчастіше комп'ютер);
- маршрутизатор (router) - пристрій, що забезпечує маршрутизацію пакетів обміну з однієї мережі в іншу;

- підмережа (subnetwork) - сукупність хостів, що є частиною мережі, для яких маршрутизатором виділено однаковий номер підмережі;
- сегмент мережі - фізична або логічне об'єднання хостів. Наприклад, бездротовий сегмент мережі утворює сукупність хостів, підключених до точки доступу за схемою «загальна шина». При такій схемі підключення кожен хост має можливість аналізувати будь-який пакет в своєму сегменті. Аналогічна картина буде спостерігатися, якщо сегмент мережі створений не фізично, а логічно (із застосуванням віртуальних мереж VLAN).

З точки зору віддаленої атаки важливе розташування зломисника і об'єкта атаки по відношенню один до одного, тобто в одному або в різних сегментах вони знаходяться. У разі всередині сегмента атаки, як впливає з назви, зломисник і об'єкт атаки знаходяться в одному сегменті. При між сегментній атаці зломисник і об'єкт атаки знаходяться в різних сегментах. Дана класифікаційна ознака дозволяє судити про так звані «ступені віддаленості» атаки.

На практиці між сегментну атаку здійснити значно важче, ніж всередині сегменту. Але між сегментна віддалена атака представляє велику небезпеку, ніж усередину сегмента атака, так як саме віддаленість порушника від об'єкта атаки може істотно перешкодити заходам по відображенню атаки.

Імовірність вдалих атак значно збільшується в разі наявності бездротових рішень. Одне з головних відмінностей між кабельними і бездротовими мережами пов'язано з тим, що здійснювати повний контроль над областю між кінцевими точками бездротової мережі досить складно. Саме цьому найбільш поширена проблема в відкритих і некерованих середовищах, таких як бездротові мережі - це можливість анонімних атак.

За співвідношенням кількості порушників і атакованих об'єктів, атака може бути віднесена до наступних класів впливу:

- вплив «один до одного» - атака здійснюється одним зломисником щодо одного об'єкта;
- вплив «один до багатьох» - атака здійснюється одним зломисником щодо кількох об'єктів;

- вплив «кілька до одного»;
- вплив «кілька до багатьох».

У двох останніх випадках атака здійснюється декількома зловмисниками з різних комп'ютерів щодо одного або декількох об'єктів (розподілений або комбінований вплив).

1.4 Соціальна інженерія як метод нападу на персональні дані

Соціальна інженерія – це такий нетехнічний тип стратегії кібератак, який базується на взаємодії між людьми та маніпуляціях таким чином, щоб людина порушила стандартні правила кібербезпеки. Для таких атак не потрібно бути хакером і знати купу технічної інформації, тому зловмисники активно використовують дану тактику. Легше обманом отримати бажане, ніж зламувати програмне забезпечення, наприклад, людина за власним бажанням передає вам свій пароль, аніж ви спробуєте зламати його. Проте соціальна інженерія вимагає від зловмисника гарної підготовки, що зазвичай має на меті збір інформації про жертву, аби точно знати, як саме можна отримати бажану інформацію.

Загрози персональним даним можна описати наступним чином - це загрози несанкціонованого зберігання, використання та поширення конфіденційних даних. За згодою суб'єкта персональних даних конфіденційна інформація може оброблятися і зберігатися розпорядником, мету в цей час визначає володілець даних. Таким чином, володілець і розпорядник несуть відповідальність за дотримання конфіденційності довіреної їм інформації. Будь-які дані зберігаються в інформаційних системах, а отже, мова про загрози персональним даним, які зберігаються та обробляються в ІС (інформаційних системах).

Усі загрози можна умовно поділити на такі, які можуть бути реалізовані внаслідок атак, та такі, які не залежать від атак.

Загрози, які не пов'язані з цілеспрямованими атаками, можуть як призвести до втрати, спотворення або компрометації персональних даних суб'єкта, так і створити умови для їх використання зловмисниками.

Такими загрозами можуть бути:

- такі, що не пов'язані з діяльністю людини: стихійні лиха та природні явища (землетруси, повені, урагани тощо);
- загрози соціально-політичного характеру: страйки, диверсії, локальні конфлікти, війна, що супроводжуються нападом на об'єкт, що містить ресурси інформаційної системи, тощо;
- помилкові дії та/або порушення персоналом та користувачами інформаційної системи вимог до відповідної експлуатаційної, організаційної, технічної чи іншої документації;
- загрози антропогенного характеру, наприклад: аварії та різного роду несправності та перешкоди, що призводять до порушень і збоїв у роботі апаратних компонентів інформаційної системи.

Закон України “Про інформацію” окреслює конфіденційну інформацію як інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою.

Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом

Захист від загроз, які не залежать від атак, регулюється інструкціями, розробленими та затвердженими уповноваженими службами розпорядника персональних даних, з урахуванням специфічних умов функціонування інформаційної системи, а також чинних нормативних документів.

Захист від загроз, які можуть бути реалізовані внаслідок атаки, повинен забезпечуватися за допомогою захисних заходів і засобів, які використовуються інформаційною системою і призначені переважно для протидії атакам.

Атака соціальної інженерії має спільну структуру. Вони відбуваються в один або кілька кроків .

На рис. схематично зображений життєвий цикл атаки.

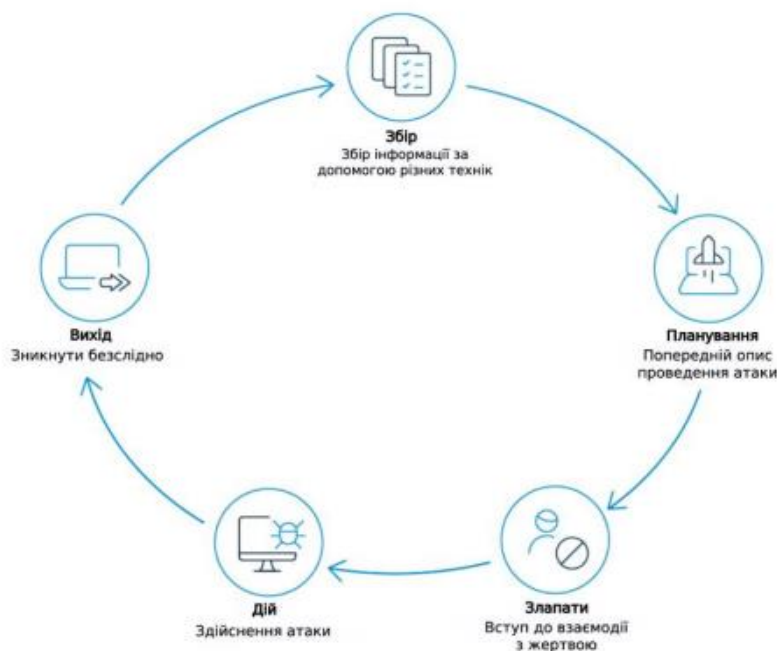


Рисунок 1.3 – Життєвий цикл атаки

Згідно цій схеми, існують наступні етапи підготовки та здійснення атаки:

1. Збір інформації та планування. Імовірність успіху більшості атак залежить саме від цієї фази, тому є логічним, що зловмисники приділяють цьому етапу більшу частину свого часу та уваги. Інформація може збиратися різними методами. Маючи правильну інформацію, зловмисник може визначити вектор атаки, можливі паролі, ймовірні відповіді окремих осіб й уточнити цілі. На цьому етапі зловмисник дуже добре ознайомлюється з жертвою та формулює конкретний план атаки під дану особу.

2. Встановлення контакту з жертвою та взаємодія. На цьому етапі зловмисник встановлює контакт з жертвою та вибудовує довірливі стосунки. Це критична точка, оскільки якість встановленого контакту визначає рівень співпраці та міру, з якою жертва буде допомагати зловмисникові досягти мети. Наприклад, це може бути доволі короткотривалий контакт, як поспішати до дверей з широкою посмішкою та зоровим контактом, щоб жертва притримала двері відкритими для зловмисника. Це може бути особисте спілкування по телефону або смол-ток з секретарем у фойє. Водночас цей етап може бути більш масштабним - таким, як побудова онлайн-знайомство та встановлення стосунків із жертвою за допомогою фальшивого профілю на сайті знайомств або в соціальних мережах.

Після цього зловмисник використовує як зібрану інформацію, так і встановлений контакт, не викликаючи підозр. Далі відбувається взаємодія зловмисника і жертви, наприклад, це може бути реалізовано шляхом розголошення, здавалося б, неважливої інформації або доступу, наданого/переданого зловмиснику. Приклади успішної фази взаємодії включають: - утримання дверей відкритими або введення зловмисника всередину приміщення; - розкриття пароля та імені користувача по телефону; - вставлення флеш-накопичувача USB із шкідливим ПЗ до комп'ютера компанії; - відкриття зараженого вкладення електронної пошти - розкриття комерційної таємниці під час обговорення з нібито «знайомим».

3. Виконання атаки. Ця фаза — це коли зловмисник досягає своєї кінцевої мети. Як правило, атака закінчується ще до того, як жертва починає розуміти, що відбувається. Натомість зловмисник має на меті закінчити атаку таким чином, щоб жертва почувалася так, ніби вона зробив щось корисне для “знайомого”, тим самим забезпечуючи можливу подальшу взаємодію.

4. Вихід з атаки. Зловмисник стирає цифрові відбитки будь-якого свого перебування. В результаті нападник досягає двох важливих цілей. По-перше, жертва не знає, що напад відбувся. По-друге, зловмисник приховує свою особу. Добре спланована і плавна стратегія виходу є метою нападника і останнім актом в атаці.

Сфера застосування соціальної інженерії достатньо широка, однак визначають основні напрямки, сфери:

- збір відкритої інформації про жертву, а саме з'ясування інтересів та особливостей поведінки потенційної жертви, соцмереж, якими вона користується, а також імен, під якими вона з'являється у мережі Інтернет, через ведення діалогу з нею або з її оточенням у службах обміну миттєвими повідомленнями;
- отримання конфіденційної інформації про об'єкт атаки або інформації, що становить для зловмисника певний інтерес, наприклад номери телефонів потенційної жертви, адресу її реєстрації, проживання, реальне ім'я та прізвище тощо, через встановлення контакту з нею або шляхом оману;

- отримання інформації про об'єкт атаки, необхідної для забезпечення несанкціонованого доступу до системи, а саме паролів, яким користується потенційна жертва, серії та номеру паспорта та інших відомостей про неї шляхом входження в довіру до обраної жертви;
- примушення жертви до дій, необхідних порушникові, через нав'язування такому об'єкту нової моделі поведінки. Наприклад. Проникнення в мережу організації для дестабілізації з певною метою роботи її основних вузлів;
- загальна дестабілізація роботи в організації з метою зниження її впливу, а згодом і повного її знищення;
- фінансові махінації в організації;
- фішинг та інші способи викрадення паролів із метою доступу до персональних даних тощо;
- викрадення клієнтських баз. Інформація про маркетингові плани організації. Загальна інформація про організацію, її сильні і слабкі ланки з метою подальшого знищення. Часто застосовується для рейдерських атак. Інформація про найбільш перспективних співробітників із метою їх подальшого переманювання до своєї організації.

Атаки соціальної інженерії не втрачають своєї популярності, з часом з'являються нові типи маніпулювання людьми, а отже і типи атак. На рис. зображені основні типи атак соціальної інженерії.



Рисунок 1.4 – Типи атак соціальної інженерії

Основне припущення які ми вводимо у роботі, це те що основним видом атаки на персональні дані будемо враховувати фішинг атаку.

Фішинг — це такий тип атак, за якого зловмисник обманним шляхом заволодіває конфіденційною інформацією. В основному зловмисники використовують даний тип атак використовуючи електронну пошту. Відтак існують найпопулярніші сценарії. Коли зловмисник надсилає фішинговий лист, він має на меті – змусити користувача виконати певні дії, щоб отримати певні дані для подальшої атаки, або ж встановити шкідливе програмне забезпечення як частину більш широкомасштабної спроби проникнення. Фішингова атака матиме більше шансів бути успішною, якщо атака персоналізована під конкретного користувач. Таким чином зловмисник створює ілюзію того, що електронний лист отриманого з надійного джерела, а отже, це підвищує ймовірність того, що користувач прочитає цей лист або навіть виконає дії згідно з рекомендаціями зловмисника. Усі фішинг атаки можуть бути поділені на 5 груп (рис 3): спрямований фішинг, полювання на корпоративних китів, телефонний фішинг, інтерактивний фішинг голосової відповіді та компромісний фішинг для ділової електронної пошти.



Рисунок 1.5 – Типи фішинг атак

Спрямований фішинг (Spear phishing) – це цілеспрямована фішингова атака. Як звичайний, так і спрямований фішинг використовують електронну пошту, щоб досягнути мети. Але у випадку спрямованого фішингу персоналізовані електронні листи надсилають конкретній особі. Перед відправленням такого електронного листа зловмисник вивчає інтереси потенційної жертви. Найчастіше жертвами спрямованого фішингу є високі посадові особи, які мають доступ до більшої конфіденційної інформації, аніж пересічний робітник.

Вішинг(англ. Vishing від поєднання Voice та Fishing) або телефонний голосовий фішинг або – це такий тип атаки, коли кіберзлочинець дзвонить за номером телефону й за допомогою створення відчуття невідкладності ситуації змушує людину вчиняти проти своїх інтересів. Такі дзвінки зазвичай відбуваються в стресовий час, наприклад, посеред ночі, коли людина раптово прокидається і має зрозуміти, що відбувається. Ці атаки є популярними, оскільки телефонні дзвінки знеособлені, оскільки жертва не бачить співрозмовника. А це надає неабиякі переваги зловмиснику, оскільки завжди можна покласти слухавку і, наприклад, викинути сім-карту. У більшості країн вже існує обов’язкова реєстрація номеру з прив’язкою до паспортних даних особи, але навіть за такого сценарію, користувач має на це певний проміжок часу до блокування сім-карти, а це дає можливість бути знеособленим деякий період.

СМС фішинг (Smishing) – це вид фішингу, який використовує текстові повідомлення на мобільних телефонах. Злочинці видають себе за офіційне джерело, щоб завоювати довіру жертви. Наприклад, під час СМС фішингу зловмисник може надіслати жертві посилання на веб-сайт. Коли жертва відвідає цей веб-сайт, на мобільний телефон буде встановлене зловмисне ПЗ. Також популярний сценарій смс-фішингу, це смсповідомлення з довільного або прихованого номеру ніби-то від банку з текстом «Vasha karta bude zablokovana bankom. Terminovo proidit avtorizaciju, abo zatelefonuite...».

Вейлінг (Whaling полювання на корпоративних китів) – це фішингова атака, що спрямована на осіб, які мають повний доступ до інформації у межах організації, наприклад, її вище керівництво. Також цілями можуть бути політики або знаменитості. Термін вейлінг походить від розміру атак, а китів вибирають відповідно до їхніх повноважень у компанії. Через чітко спрямований характер вейлінг-атаки часто важче виявити, ніж стандартні фішинг-атаки. На підприємстві адміністратори безпеки можуть допомогти знизити ефективність вейлінг-атак, залучаючи співробітників корпоративного управління пройти навчання з інформаційної безпеки.

Інтерактивний фішинг голосової відповіді виконується за допомогою інтерактивної системи голосового реагування, щоб жертва вводила приватну інформацію так, ніби вона отримала дзвінок від знайомого бізнесу або банку.

1.5 Необхідність розробки системи аналізу захищеності інформації в інформаційно-комунікаційних системах і мережах

В організації, що використовує корпоративну інформаційну систему, потрібно регулярно перевіряти, наскільки реалізовані або використовувані механізми захисту інформації відповідають положенням прийнятої в організації політики безпеки. Таке завдання періодично виникає при зміні і оновленні компонентів інформаційної системи, зміні конфігурації операційної системи і тому подібне. Використання засобів аналізу захищеності дозволяє визначити уразливості на вузлах корпоративної мережі і усунути їх до того, як ними скористаються зловмисники.

Засоби аналізу захищеності працюють на початковому етапі здійснення атаки. Виявляючи і своєчасно усуваючи уразливості, вони тим самим запобігають самій можливості реалізації атаки, що дозволяє понизити витрати (фінансові, ресурсні, людські і так далі) на експлуатацію засобів захисту. Технології аналізу захищеності є дієвим методом, що дозволяє проаналізувати і реалізувати політику мережевої безпеки перш, ніж здійсниться спроба її порушення зовні або зсередини організації. Засоби аналізу захищеності можуть функціонувати на мережевому рівні, рівні операційної системи (ОС) і рівні застосування. Вони можуть проводити пошук уразливостей, поступово нарощуючи число перевірок і "поглиблюючись" в інформаційну систему, досліджуючи усі її рівні.

Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів. Обумовлено це в першу чергу універсальністю використовуваних протоколів. Вивченність і повсюдне використання таких протоколів, як IP, TCP, HTTP, FTP, SMTP і тому подібне, дозволяють з високою мірою ефективності перевіряти захищеність інформаційної системи, що працює в мережевому оточенні.

Другими за поширеністю є засоби аналізу захищеності операційних систем. Обумовлено це також універсальністю і поширеністю деяких операційних систем (наприклад, UNIX і Windows NT). Проте, через те, що кожен виробник вносить до операційної системи свої зміни (як приклад можна привести велику кількість різновидів ОС UNIX), засоби аналізу захищеності ОС аналізують в першу чергу параметри, характерні для всього сімейства однієї ОС. І лише для деяких систем аналізуються специфічні для неї параметри.

Засобів аналізу захищеності застосувань на сьогодні не так вже багато. Такі засоби доки існують тільки для широко поширених прикладних систем типу: Web-браузери (Netscape Navigator, Microsoft Internet Explorer), СУБД (Microsoft SQL Server, Oracle) і тому подібне.

В 2018 році в Євросоюзі введений в дію Загальний регламент щодо захисту даних (англ. General Data Protection Regulation, GDPR), що вимагає від кожної організації в будь-який момент часу на усіх ділянках власної діяльності або ланцюга поставок, продемонструвати, які персональні дані і для яких цілей є в наявності, як вони обробляються, зберігаються і захищаються. При чому ці відомості повинні бути надані не тільки в ході перевірок уповноваженими органами, а й на вимогу приватної особи – власника цих даних.

Дотримання такого комплексу дій вимагає від компанії значних затрат коштів і ресурсів. І хоча в порядкування обробки персональних даних передбачає в довгостроковій перспективі поліпшення інформаційної безпеки, в короткостроковому плані ризики організації помітно зростають.

Найбільше зміна, яке відбудеться в організації після імплементації GDPR, буде не поява нових правил і політик, а перегляд ставлення до персональних даних та їх захист, а саме: компанії відчують більшу відповідальність за збір, обробку та зберігання даних; розробка продукту або сервісу буде починатися з продумування і оцінки впливу і ризиків для даних вже до, а не після релізу; кожен співробітник, який має доступ до персональної інформації буде обізнаний про правила і тому буде вже усвідомлено піклуватися про збереження персональних даних, тим самим дотримуючись базових правил щодо їх захисту.

Для перевірки захищеності інформаційних систем існують програмні продукти класу "сканер безпеки системи". Ці продукти на сьогоднішній день існують для більшості операційних систем. Найвідоміші: ASET (компонент ОС Solaris), KSA (для платформ NetWare і NT), SSS (System Security Scanner) (Unix-платформи).

System Security Scanner

Програма System Security Scanner призначена для проведення перевірки стану безпеки на окремих UNIX-комп'ютерах і пошуку уразливості ОС як зовні (по мережі з використанням Internet Scanner), так і зсередини (з самої ОС комп'ютера). При цьому проводиться перевірка прав доступу і прав власності файлів, конфігурацій мережних сервісів, установок ресурсів користувачів, програм аутентифікації і інших, пов'язаних з користувачами слабких місць (наприклад, паролів).

Пакет програм Internet Scanner SAFEsuite призначений для проведення комплексної оцінки ефективності політики безпеки на рівні мережних сервісів. Він надає можливості для ідентифікації і корекції більше 140 відомих слабких місць і постійного нагляду за станом безпеки для широкого діапазону мережних пристроїв - від web-вузлів і міжмережевих екранів і до серверів і робочих станцій UNIX, Windows 95, Windows NT і всіх інших пристроїв працюючих з TCP/IP. Складається з трьох програм: Web Security Scanner, Firewall Scanner, Intranet Scanner.

- Web Secure Scanner Призначений для пошуку слабких місць безпеки на web-серверах. Забезпечує аудит ОС, під управлінням якої працює web-сервер, програм-додатків, встановлених на web-сервері, і CGI scripts в web-приложениях. Проводить тестування конфігурації web-сервера, оцінює рівень безпеки основної файлової системи.

- Firewall Scanner Забезпечує пошук слабких місць в міжмережевих екранах, перш за все в їх конфігурації, і надає рекомендації по їх корекції. Проводить тестування реакції міжмережевих екранів на різні типи спроб порушення безпеки. Виконує сканування сервісів - ідентифікацію всіх мережних сервісів, доступ до яких здійснюється через міжмережевий екран.

- Intranet Scanner Призначений для автоматичного виявлення потенційних слабких місць усередині мереж з використанням різних тестів для перевірки реакції на несанкціоновані проникнення. Забезпечує перевірку різних мережних пристроїв, включаючи UNIX hosts, системи, що працюють під Microsoft NT/Windows 95, маршрутизатори, web-сервери і X-терминалы.

Сімейство продуктів SAFEsuite, розроблених американською компанією Internet Security Systems (ISS) - комплект засобів призначених для оцінки захищеності інформаційних систем. Складається з системи аналізу захищеності на рівні мережі Internet Scanner, засобу аналізу захищеності на рівні хосту System Scanner і виявлення атак на рівні мережі RealSecure Network Engine, Database Scanner.

Система аналізу захищеності — Internet Scanner — призначена для проведення регулярних всесторонніх або вибіркових тестів мережних служб, операційних систем, прикладного, що використовується, ПО, маршрутизаторів, міжмережевих екранів, Web-серверов і т.п. Результатом тестування є звіти, що містять докладний опис кожної знайденої уразливості, її дислокації в корпоративній мережі, а також рекомендації по корекції або усуненню «слабкого місця».

Система аналізу захищеності Database Scanner призначена для виявлення проблем, пов'язаних з безпекою баз даних. В цьому ПО реалізовані перевірки підсистем аутентифікації, авторизації і контролю цілісності. Вбудована база знань, містить перелік коректуючих дій, що рекомендуються, для усунення знайдених уязвимостей.

Database Scanner підтримує СУБД Microsoft SQL Server, Sybase Adaptive Server, Oracle, Informix.

РОЗДІЛ 2 ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В ІТС

2.1 Захист персональних даних від атак за допомогою алгоритмів соціальної інженерії

Виявлення фішингових атак Можливо виокремити два основних підходи до виявлення фішингу: навчання користувачів і за допомогою програмних засобів.

1) Навчання користувачів: користувачів можна навчити краще розуміти природу фішингових атак, що в результаті допоможе коректно розрізняти фішингові і справжні повідомлення. Це суперечить категоризації в роботі, де навчання користувачів розглядається як превентивний захід. Однак навчання має на меті розпізнавання користувачами фішингових атак, тому розглядається як підхід до виявлення фішингу.

2) За допомогою програмних засобів: цей підхід має на меті заповнити прогалину, яка виникає через помилку користувача або незнання, та розрізняти програмним способом фішингові та легітимні повідомлення. Цей недолік вимагає вирішення, оскільки навчання користувачів є дорожчим, ніж автоматична класифікація, та не завжди є можливим, наприклад, коли бази користувачів є завеликими (PayPal, eBay, Amazon тощо).

Розпізнавання фішингової атаки – це початкова точка протидії фішинговим атакам. На рис. показана схема підходів до розпізнавання фішингових атак.

Ефективність виявлення може бути покращена за рахунок навчання класифікатора (як людини, так і ПЗ). У випадку з навчанням користувачів якість виявлення може бути покращена за рахунок їхнього індивідуального досвіду або за допомогою зовнішніх навчальних програм. У випадку програмної класифікації ефективність може бути підвищена в процесі в процесі “навчання” класифікатора, побудованого на алгоритмах машинного навчання, або вдосконаленням правил виявлення в системі на основі правил.

Програмний підхід до виявлення

Чорні списки. Це постійно оновлюванні списки, що містять раніше виявлені фішингові URL-адреси. Недоліком даної методології є затримка в оновленні

списків. Для того, щоб щойно створений фішинговий сайт потрапив у список, необхідний час. Цієї затримки між відправленням даних і додаванням сайту до списку може бути достатньо для досягнення зловмисниками своїх цілей.



Рисунок 2.1 – Розпізнавання фішингу

Білі списки. Ці списки є чимось протилежним до чорних. Якщо є певна URLадреса, її порівнюють з легітимною адресою зі базою даних “білого списку”. База даних «білого списку» здебільшого містить список популярних справжніх URL-адрес та їхні важливі дані. Як і у випадку з чорним списком, для завантаження нової відомої URLадреси може знадобитися певний час, через який, зловмисник, безсумнівно, може досягти своїх цілей.

Евристичні методи виділяють певні характеристики веб-сторінки для того, щоб визначити легітимність веб-сайту, а не залежати від будь-яких попередньо скомпільованих списків. Це перевага евристичних методів, над “списками”. Більшість цих характеристик витягуються з URL-адреси та дерево об’єктної моделі документа HTML (DOM) даної веб-сторінки. Вилучені характеристики порівнюються з вже відомими, що були зібрані з фішингових та справжніх сторінок, щоб визначити їх легітимність. Деякі з цих підходів використовують евристики для обчислення оцінки підробки даної веб-сторінки, щоб перевірити її справжність. Сучасні веб-браузери та поштові клієнти побудовані з механізмами захисту від фішингу, такими як евристичні тести з метою виявлення фішингових атак. Так само евристичні тести виявлення фішингу можуть бути включені в антивіруси.

Методи візуальної схожості. Це методи розрізнення фішингових сайтів та легітимних сайтів за зовнішнім виглядом сайтів. Зазвичай фішингові сайти є майже точними копіями справжніх, щоб у користувача не виникали сумніви щодо легітимності ресурсу. З метою не бути виявленими зловмисники, як правило, вставляють зображення, Flash, ActiveX і Java-аплет замість HTML-тексту. Методи виявлення на основі візуальної схожості можуть швидко розпізнавати перераховані об'єкти на веб-сторінках фішингових сайтів. Методи, засновані на візуальній схожості, використовують підпис, щоб розрізняти фішингові сторінки. Щоб зробити підпис потрібно вибирати спільні компоненти з усього сайту, а не з окремої сторінки веб-сайту. Таким чином, одного підпису достатньо, щоб ідентифікувати різні цільові веб-сторінки окремого веб-сайту або унікальні форми веб-сайту. Даний метод використовує для порівняння дерево об'єктної моделі документа HTML (DOM), схожість каскадної таблиці стилів (CSS), візуальне сприйняття, візуальні особливості, піксельні та гібридні підходи.

Машинне навчання забезпечує спрощені та ефективні методи аналізу даних, останнім часом демонструючи багатообіцяючі результати у проблемах класифікації в реальному часі. Ключовою перевагою машинного навчання є можливість створювати гнучкі моделі для конкретних завдань, таких як виявлення фішингу. Оскільки фішинг є проблемою класифікації, моделі машинного навчання можна використовувати як потужний інструмент. Моделі машинного навчання можуть швидко адаптуватися до змін.

2.2 Антивірусні технології

Шкідливе програмне забезпечення (ШПЗ) або шкідлива програма – це код, який виконує шкідливі дії; він може прийняти форму виконавчого файлу, скрипта, коду або будь-якого іншого програмного забезпечення (ПЗ). Зловмисники використовують ШПЗ для крадіжки конфіденційної інформації, для шпигування за зараженою системою або з метою взяти систему під контроль. Нижче наведені деякі шкідливі дії, що виконуються ШПЗ:

- порушення роботи комп'ютера;
- крадіжка конфіденційної інформації;

- несанкціонований доступ до системи жертви;
- шпигунство;
- посилення спам-листів;
- участь в DDoS атаках;
- блокування файлів на комп'ютері та утримання їх з метою викупу.

Проаналізувавши різні джерела можна виділити таку класифікацію ШПЗ, яку представлено у вигляді схеми

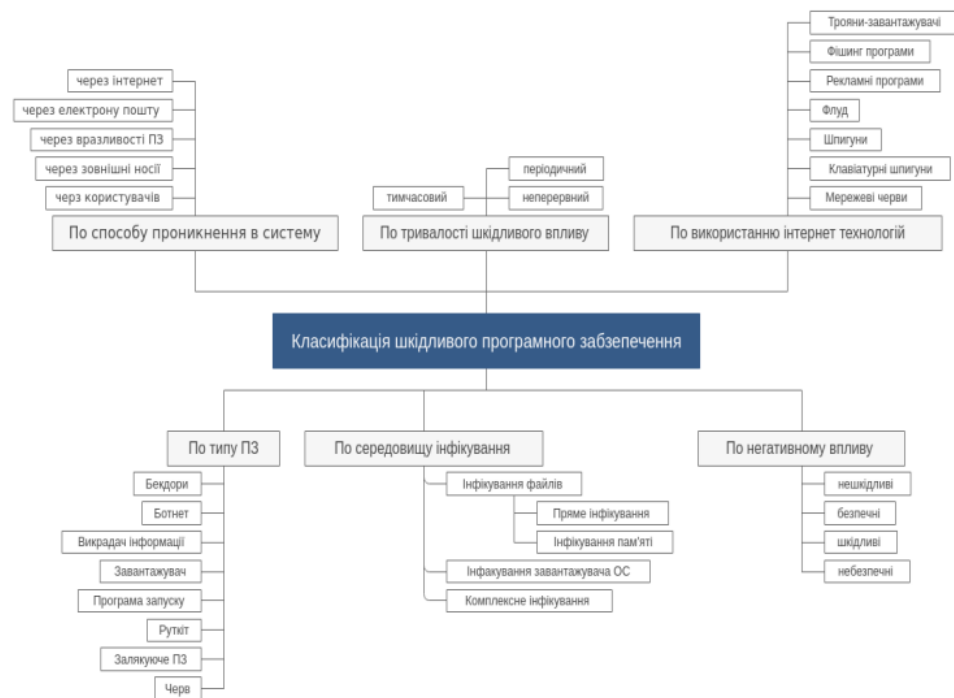


Рисунок 2.2 – Класифікація шкідливого програмного забезпечення

Методи боротьби з ШПЗ:

- виявлення ШПЗ;
- блокування роботи ШПЗ;
- усунення наслідків дії ШПЗ. Виявлення ШПЗ бажано здійснювати на стадії його впровадження або, принаймні, до початку здійснення деструктивних функцій ШПЗ. Усунення наслідків дії ШПЗ ведеться у двох напрямках:

- видалення ШПЗ;
- відновлення (при необхідності) файлів, областей пам'яті. Відновлення системи залежить від типу ШПЗ, а також від елементу часу виявлення ШПЗ по відношенню до початку деструктивних дій.

Методи виявлення ШПЗ:

– сканування. Сканування – один з найпростіших методів виявлення ШПЗ. Сканування здійснюється програмою-сканером, яка проглядає файли у пошуках пізнавальної частини ШПЗ – сигнатури. Програма фіксує наявність вже відомого ШПЗ, за винятком поліморфного ШПЗ, які застосовують шифрування тіла вірусу, змінюючи при цьому кожного разу і сигнатуру. Програми-сканери можуть зберігати не сигнатури відомого ШПЗ, а його контрольну суму. Програмисканери часто можуть видаляти знайдене ШПЗ. Такі програми називаються поліфагами. Метод сканування застосовується для виявлення ШПЗ, сигнатури якого вже виділені і є постійними. Для ефективного використання методу необхідне регулярне оновлення відомостей про нове ШПЗ.

– виявлення змін. Метод виявлення змін базується на використуванні програм-ревізорів. Ці програми визначають і запам'ятовують характеристики всіх областей на дисках, в яких звичайно розміщується ШПЗ. При періодичному виконанні програм-ревізорів порівнюються характеристики, що зберігаються, і характеристики, одержувані при контролі областей дисків. За наслідками ревізії програма видає відомості про можливу наявність вірусів. Звичайно програмиревізори запам'ятовують в спеціальних файлах образи головного завантажувального запису, завантажувальних секторів логічних дисків, характеристики всіх контрольованих файлів, каталогів і номери дефектних кластерів. Можуть контролюватися також обсяг встановленої оперативної пам'яті, кількість підключених до комп'ютера дисків і їх параметри. Головною перевагою методу є можливість виявлення ШПЗ всіх типів, а також нового і невідомого ШПЗ. Досконалі програми-ревізори знаходять навіть стелс-віруси. Є у цього методу і недоліки. За допомогою програм-ревізорів неможливо визначити ШПЗ у файлах, які поступають в систему вже зараженими. ШПЗ буде знайдене тільки після розмноження в системі. Програми-ревізори непридатні для виявлення зараження ресурсів, оскільки документи і таблиці дуже часто змінюються.

– евристичний аналіз. Евристичний аналіз порівняно недавно почав використовуватися для виявлення ШПЗ. Як і метод виявлення змін, даний метод дозволяє визначати невідоме ШПЗ, але не потребує попереднього збору, обробки і

зберігання інформації про файлову систему. Суть евристичного аналізу полягає в перевірці можливих середовищ існування ШПЗ і виявлення в ньому команд (груп команд), характерних для ШПЗ. Такими командами можуть бути команди створення резидентних модулів в оперативній пам'яті, команди прямого звернення до дисків, минувши ОС. Евристичні аналізатори при виявленні «підозрілих» команд у файлах або завантажувальних секторах видають повідомлення про можливе зараження. Після отримання таких повідомлень необхідно ретельно перевірити ймовірно заражені файли і завантажувальні сектори всіма наявними антивірусними засобами

- використання резидентних сторожів. Метод використання резидентних сторожів заснований на застосуванні програм, які постійно знаходяться в ОП ЕОМ і відстежують всі дії решти програм. У разі виконання якою-небудь програмою підозрілих дій (звернення для запису в завантажувальні сектори, переміщення в ОП резидентних модулів, спроби перехоплення переривань і т. п.) резидентний сторож видає повідомлення користувачу. Програма-сторож може завантажувати на виконання інші антивірусні програми для перевірки «підозрілих» програм, а також для контролю всіх файлів (із змінних дисків, флешек, по мережі), що поступають ззовні. Істотним недоліком даного методу є значний відсоток помилкових повідомлень, що заважає роботі користувача, викликає роздратування і бажання відмовитися від використання резидентних сторожів.

- вакцинація програм. Під вакцинацією програм розуміється створення спеціального модуля для контролю її цілісності. Як характеристика цілісності файлу, зазвичай використовується контрольна сума. При зараженні вакцинованого файлу, модуль контролю знаходить зміну контрольної суми і повідомляє про це користувача. Метод дозволяє знаходити все ШПЗ, у тому числі і невідоме, за винятком стелсвірусів.

- апаратно-програмний захист від вірусів.

2.3 Технології виявлення та блокування кібератак на кінцевих пристроях

Gartner визначає Endpoint Threat Detection and Response (EDR) як інструмент для детектування і розслідування підозрілих активностей (і їх слідів) на кінцевих точках. Таким чином, цей клас рішень може бути віднесений до продуктів сімейства Advanced Threat Protection. Архітектурно схема роботи рішення виглядає таким чином: агент на кінцевій точці відстежує події на рівні системи і мережі, і або відправляє інформацію про них на сервер або хмару для подальшого аналізу, або локально проводить аналіз, дозволяючи оперативно відреагувати на виявлені загрози. Технології машинного навчання і поведінкового аналізу, а також інтеграція з потоками Threat Intelligence, дозволяють виявляти невідомі загрози і надавати розширені інструменти для розслідування інцидентів і побудови звітів.

Сучасні рішення класу EDR дозволяють:

- забезпечувати моніторинг кінцевих точок в режимі реального часу і представляти наочну візуалізацію активностей всіх робочих станцій і серверів в корпоративній інфраструктурі з єдиної консолі;
- ефективно виявляти і пріоритезувати інциденти інформаційної безпеки в міру їх виникнення на кінцевих точках;
- записувати і зберігати інформацію по активностей на кінцевих точках для подальшого розслідування комплексних інцидентів;
- надавати необхідну інформацію фахівцям ІБ для оперативного розслідування інцидентів;
- реагувати на інциденти, забезпечуючи їх стримування, а також допомагають у відновленні робочих станцій у вихідне до інциденту стан;
- підтримувати можливість взаємодії з рішеннями класу EPP.



Рисунок 2.3 – Сучасні рішення класу EDR

Наочність. Рішення EDR дозволяє проводити спостереження за всіма діями кінцевих точок, наприклад, встановлення нового програмного забезпечення, скачування файлів, підвищення рівня привілеїв облікових записів, а також зміни в запущених процесах, в мережевій активності, в поведінці користувачів та ін.

Виявлення. Вкрай важливо якнайшвидше виявити атаку, що розвивається, до того, як вона завдасть серйозної шкоди організації. Рішення EDR дозволяють виявити складні атаки на їх ранніх стадіях, використовуючи комбінацію різних механізмів пошуку і методів аналізу невідомих загроз, в тому числі побудованих на базі машинного навчання і поведінкового аналізу.

Методи виявлення:

- ІоС-сканування;
- антивірусний захист;
- виявлення аномальної поведінки;
- пісочниця;
- розвідка загроз;
- ретроспективний аналіз;
- кореляція.

Розслідування. Швидкий доступ до всіх даних з кінцевих точок і до інформації про активність дозволяє аналітикам виконувати комплексне розслідування і глибокий аналіз джерел загроз. EDR надає докладні відомості про будь-які виявлені загрози, наприклад, як загроза проникла в інфраструктуру організації; список порушених робочих станцій і серверів; інформація про зміни в порушених атакою кінцевих точках; застосунки, що запускаються; створені в ході атаки файли; завантажені файли та ін.

Реагування. Широкий набір інструментів дозволяє фахівцям з інформаційної безпеки переглядати події, оцінювати масштаб порушень і визначати всі порушені кінцеві точки. Рішення EDR дозволяють забезпечувати стримування складних інцидентів, усуваючи загрози на окремих кінцевих точках, і їх наслідки без впливу на роботу користувачів. Під час реагування здійснюється:

- зупинка запущених шкідливих процесів;
- карантин файлів;
- ізолювання заражених робочих станцій;
- проведення необхідних віддалених дій з файлами та реєстром;
- блокування підключень кінцевих точок до зловмисних доменів, URL- і IP-адресами;
- збір криміналістичних артефактів (образів оперативної пам'яті, образів жорсткого диска);
- відновлення робочих місць в стан що був до зараження.

User [and Entity] Behavioral Analytics (UEBA / UBA) - клас систем, що дозволяють на основі масивів даних про користувачів та ІТ-сутності (кінцевих станціях, серверах, комутаторах, тощо) за допомогою алгоритмів машинного навчання і статистичного аналізу будувати моделі поведінки користувачів і визначати відхилення від цих моделей, як в режимі реального часу, так і ретроспективно.

Як джерела даних для UEBA-систем можуть виступати файли журналів серверних і мережевих компонентів, журнали систем безпеки, локальні журнали з

кінцевих станцій, дані з систем аутентифікації і навіть зміст листування в соціальних мережах, месенджерах і поштових повідомленнях.

Системи UEBA представлені як у вигляді окремих програмних рішень, так і у вигляді розширень для вже існуючих систем: SIEM (Security Information and Event Management), DLP (Data Loss Prevention), EDR (Endpoint Detection and Response) та ін.

Системи UEBA, архітектурно, вирішують 4 основні завдання:

- Збір даних з різних джерел, здійснення як простого статистичного, так і розширеного аналізу, з використанням методів машинного навчання, в режимі реального часу і/або з певною періодичністю.
- Швидка ідентифікація атак і інших порушень, більшість з яких не визначаються класичними засобами ІБ.
- Пріоритизація подій, консолідованих з різних джерел (SIEM, DLP, AD, тощо), для більш оперативного реагування з боку адміністраторів ІБ.
- Більш ефективна реакція на події за рахунок надання адміністраторам ІБ розширеної інформації про інцидент, що включає всі об'єкти, які були залучені в аномальну активність.

В ядро будь-якої UEBA-системи включаються технології по роботі з великими масивами даних. І якщо у випадку з розширеннями до відомих SIEM-систем (IBM QRadar UBA, HPE ArcSight UBA, LogRhythm AI Engine) такі технології доступні з коробки, то самостійні рішення повинні або використовувати сторонні розробки (наприклад, Exabeam використовує Elastic Stack), або свої власні (Splunk UBA, Microsoft ATA). UEBA здатні доповнювати широкий клас ІБ-систем і вирішувати завдання, які ці системи не можуть вирішити в принципі:

- Визначення скомпрометованих акаунтів користувачів і кінцевих станцій.
- Визначення та запобігання інсайдерських загроз.
- Моніторинг співробітників і їх прав доступу.

2.4 Технології протидії витокам інформації

Системи захисту від витоків конфіденційної інформації (DLP) - це системи, що дозволяють в режимі реального часу проводити моніторинг і блокування

вхідних і вихідних повідомлень співробітників, відправлення файлів на зовнішні носії, мережеві сховища інформації та веб-ресурси, а також контроль голосових і текстових повідомлень, переданих по протоколу SIP, з метою запобігання витоку конфіденційної інформації.

Порушення конфіденційності (як випадкове, так і навмисне) може спричинити втрату довіри клієнтів і партнерів, удар по репутації компанії, зниження її конкурентоспроможності та прямі фінансові збитки. Доступ з робочого місця до популярних сервісів веб-пошти, соціальних мереж і месенджерів збільшує ризик витоків конфіденційної інформації. При цьому блокування цих ресурсів провокує співробітників шукати нові обхідні шляхи комунікації, підвищуючи свою технічну грамотність.

Ефективним засобом контролю інформаційних ресурсів є комплекс організаційних заходів, розроблених регламентів і технічні засоби, що дозволяють контролювати і забезпечувати їх дотримання. До них відносяться системи класу DLP (Data Leak Prevention, захист від витоків інформації). Під «витоком» в даному випадку розуміється порушення конфіденційності важливої інформації.

Системи DLP це технології, що дозволяють запобігти витоку конфіденційної інформації. У перебігу останніх декількох років використовувалася велика термінологія: Information Leakage Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS) та ін. Але остаточною і найбільш точним терміном прийнято вважати Data Leak Prevention (DLP, запропонований агентством Forrester в 2005 г.).

Функціонал DLP-систем включає в себе моніторинг інформації, що передається співробітниками в інтернет, і контроль даних, що зберігаються на внутрішніх загальнодоступних ресурсах компанії, робочих станціях користувачів і копіюються на зовнішні носії. На сьогоднішній день DLP-рішення, як правило, мають у своєму розпорядженні широкі можливості для контролю інформації, засновані на контентному аналізі і більш складних алгоритмах (наприклад, цифрових відбитках, пошуку ідентифікаторів та ін.).

Архітектура DLP-системи

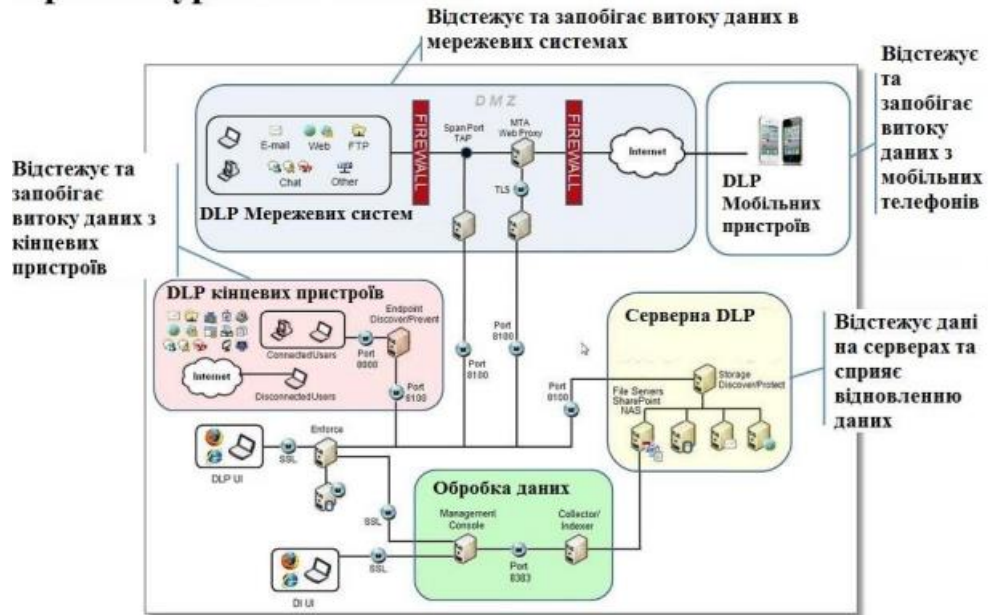


Рисунок 2.5 – Архітектура DLP-системи

Системи захисту від витоків конфіденційної інформації виконують такі завдання:

- Зберігання копій конфіденційної інформації, що передається засобами електронної пошти, месенджерів і IP-телефонії, що відправляється на зовнішні носії та мережеві корпоративні та веб-ресурси, з метою подальшого розслідування інцидентів інформаційної безпеки в організації.
- Блокування передачі конфіденційної та іншої небажаної інформації за межі компанії.
- Блокування передачі невідповідної інформації у внутрішній мережі компанії.
- Блокування можливості використання співробітниками ресурсів організації в особистих цілях.
- Пошук місць розташування несанкціонованих копій конфіденційної інформації (пошук конфіденційних даних).

Крім цього, DLP-системи можуть використовуватися в якості систем контролю дій співробітників - контролювати їх присутність на робочому місці, відстежувати їх лояльність і благонадійність.

Шлюзові DLP-системи засновані на використанні шлюзів - централізованих серверів обробки мережевого трафіку, що на них надсилається. Область використання таких рішень обмежена самим принципом їх роботи. Іншими словами, шлюзові системи дозволяють захищатися лише від витоків інформації через протоколи, використовувані в традиційних інтернет-сервісах: HTTP, FTP, POP3, SMTP та ін. При цьому контролювати те, що відбувається на кінцевих точках корпоративної мережі з їх допомогою неможливо.

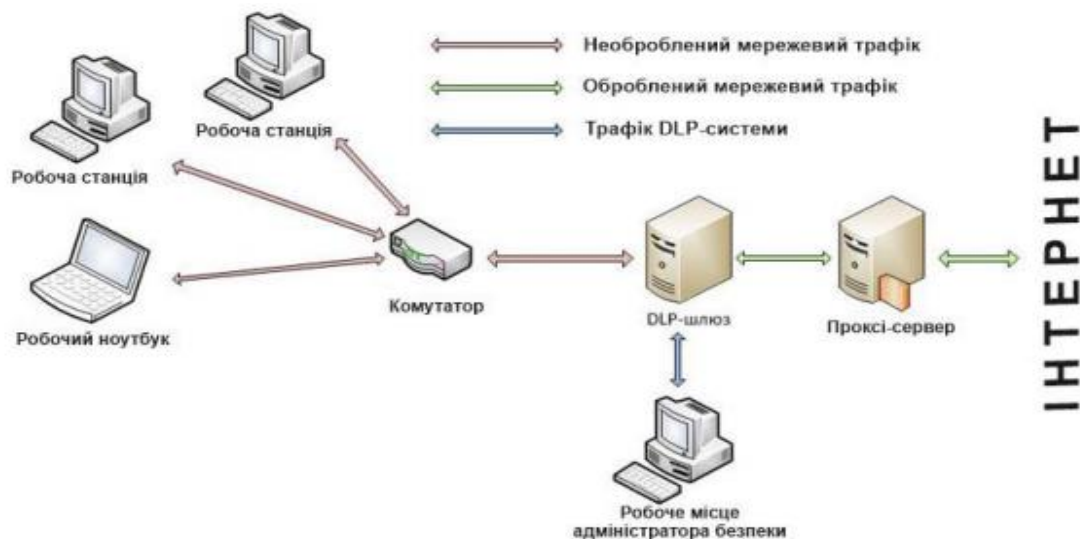


Рисунок 2.6 – Шлюзова DLP-системи, що працює в режимі блокування



Рисунок 2.7 – Шлюзова DLP-системи, що працює в режимі моніторингу

Хостові DLP-системи засновані на використанні спеціальних агентів, які встановлюються на кінцевих точках корпоративної мережі. Ці програми грають

відразу дві ролі. З одного боку вони контролюють діяльність користувачів комп'ютерів, не дозволяючи їм виходити за рамки встановленої політики безпеки (наприклад, забороняючи копіювати будь-які файли на "флешки"). А, з іншого, реєструють всі дії операторів і передають їх в централізоване сховище, дозволяючи співробітникам відділу інформаційної безпеки отримати повну картину того, що відбувається. Використання програм-агентів обмежує сферу застосування хостових DLP-систем: вони здатні бачити лише локальні або мережеві пристрої, підключені безпосередньо до тих комп'ютерів, на яких вони працюють.

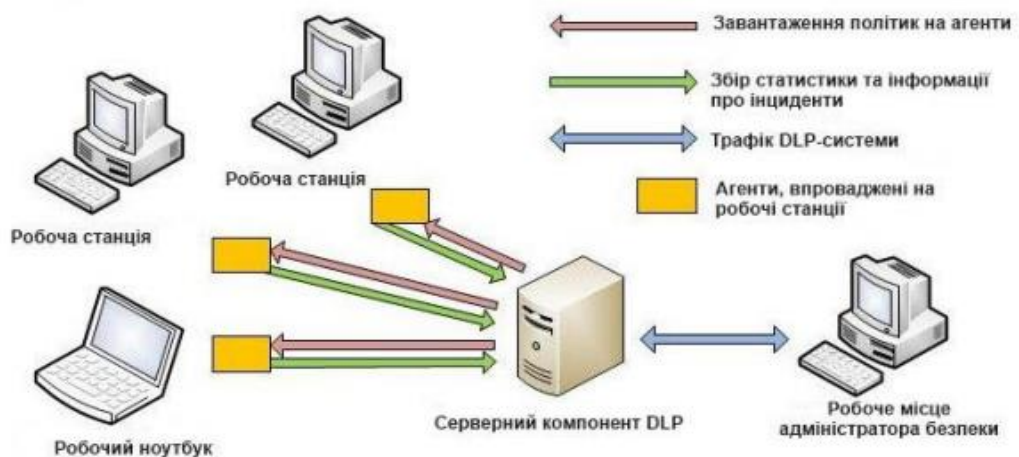


Рисунок 2.8 – Хостові DLP-системи

2.5 Технологія обману в захисті ІТС

Призначення технології обману полягає в тому, що вона допомагає досягти будь-яких або всіх наступних чотирьох цілей безпеки:

- Увага – увагу противника може бути перенаправлено від реальних активів до фальшивих.
- Енергія – цінний час і енергію зловмисника можна витратити на фейкові цілі.
- Упевненість у собі – невизначеність може бути створена навколо правдивості виявленої вразливості.
- Аналіз – може бути створена основа для аналізу безпеки в реальному часі поведінки супротивника.

Deception technologies – сукупність технік імітації ІТ-інфраструктури та дезінформації зловмисників, які використовуються з метою:

- порушення засобів автоматизації зловмисника та затримки його дій або ж порушення прогресу атаки;
- виявлення та уповільнення просування атак зловмисників, що в результаті дозволяють зупиняти атаки до нанесення значного збитку;
- звернення уваги зловмисника на себе, щоб відвернути його від реальних ресурсів, при цьому зібрати інформацію про місцезнаходження зловмисника, його інструменти і методи атак. Обман в цьому контексті використовується в якості техніки для оборонних або підривних цілей і не має протизаконного характеру.

2.6 Технології механізму безпечного виконання програм

Пісочниця (англ. Sandbox) — механізм для безпечного виконання програм. Пісочниці часто використовують для запуску непротестованого коду, неперевіреного коду з ненадійних джерел, а також для запуску та виявлення вірусів. Пісочниця — це, зазвичай, жорстко контрольований набір ресурсів (місце на жорсткому диску та в оперативній пам'яті) для виконання гостьової програми. Доступ до мережі, системних ресурсів операційної системи, пряме зчитування інформації з пристроїв введення найчастіше або частково емулюються, або сильно обмежуються. Пісочниці є прикладом віртуалізації.

Підвищена безпека виконання коду в пісочниці передбачає захист системи від великих навантажень — саме тому деякі види пісочниць використовують для запуску невідлагодженого або шкідливого коду.

Fortinet FortiSandbox — це потужна пісочниця, яка використовує машинне навчання (ML) для виявлення та усунення загроз у режимі реального часу. Вона аналізує підозрілий контент, включаючи мережевий трафік, файли, URL-адреси та іншу потенційно шкідливу активність. FortiSandbox легко інтегрується з існуючими технологічними рішеннями, автоматизуючи процес виявлення та перевірки підозрілого контенту. FortiSandbox використовує двоетапний процес високої точності верифікації файлів. Спочатку підозрілі файли звіряються з базою даних відомих загроз, що дозволяє швидко виявити та заблокувати відоме шкідливе ПЗ. Потім файл аналізується у логічно ізольованому середовищі, де алгоритми

машинного навчання визначають ознаки атак. Такий динамічний двоетапний підхід забезпечує як ефективність, так і швидкість роботи рішення.

Symantec Sandbox З 1982 року компанія Symantec від Broadcom розробляє широкий спектр рішень для забезпечення безпеки та підвищення продуктивності підприємств. Їхнє рішення Content Analysis and Sandboxing відстежує мережевий трафік, виявляючи підозрілі активності та спрямовуючи їх у пісочницю для більш глибокого аналізу. Платформа використовує Symantec Proxy, власний аналізатор шкідливого програмного забезпечення з функцією подвійної пісочниці, який перевіряє трафік на кількох рівнях для точного виявлення загроз.

Рішення виявляє індикатори компрометації (IOCs) та передає цю інформацію до інструментів захисту кінцевих пристроїв, що дозволяє проводити точні та ефективні заходи щодо усунення загроз. Завдяки пріоритезації повідомлень адміністратори отримують попередження лише про реальні загрози, що знижує втому від надлишкових сигналів та прискорює час реагування. Платформа проста в налаштуванні та масштабується разом із зростанням організації, забезпечуючи постійний захист.

Trellix - світовий постачальник рішень в галузі кібербезпеки, широко відомий своєю XDR-платформою. Сьогодні Trellix захищає понад 40 000 корпоративних та державних клієнтів у всьому світі. Платформа не обмежується виявленням та пісочницею, пропонуючи також просунутий аналіз шкідливого ПЗ та можливість ділитися розвідданими про кіберзагрози з іншими елементами ІТ-інфраструктури. Це дозволяє швидко реагувати на погрози, блокувати командні сервери, ізолювати скомпрометовані системи та запобігати подальшим атакам. Рішення поєднує статичний аналіз коду, динамічний аналіз та машинне навчання для всебічного захисту від загроз. Trellix Advanced Threat Defense легко інтегрується з іншими інструментами безпеки за допомогою REST API. Платформа відповідає високим стандартам безпеки і підтримує такі формати, як STIX (Structured Threat Information eXpression) та TAXII (Trusted Automated eXchange of Indicator Information). Зручний інтерфейс та наочні візуалізації стану мережі роблять використання платформи інтуїтивно зрозумілим.

Trend Micro Deep Discovery. Trend Micro є провідним постачальником рішень для кібербезпеки підприємств, що пропонує широкий спектр продуктів, включаючи захист хмари, мережі, кінцевих пристроїв та XDR-сервіси. Інструмент Deep Discovery Analyzer від Trend Micro створює віртуальні образи конфігурацій кінцевих пристроїв, що дозволяє точно оцінити вплив шкідливого програмного забезпечення на мережу. Рішення відрізняється гнучкістю: за його допомогою можна керувати до 60 пісочницями на одному пристрої. Deep Discovery Analyzer виходить за рамки традиційних технологій пісочниці, передаючи зібрані дані іншим інструментам Trend Micro для протидії різним типам атак. Платформа ретельно відстежує мережевий трафік, що дозволяє швидко проводити розслідування підозрілого контенту. Крім того, вона виконує просунутий аналіз URL та вмісту документів з використанням евристичних, статичних та поведінкових методів виявлення.

Zscaler, зі штаб-квартирою в Сан-Хосе, надає рішення для хмарної безпеки та пропонує два ключові продукти: Zscaler Internet Access та Zscaler Private Access. Платформа використовується у більш ніж 185 країнах, що дозволяє Zscaler ефективно виявляти загрози завдяки широким даним. Одним з основних інструментів Zscaler Internet Access є хмарна пісочниця, яка використовує ШІ для карантину та аналізу загроз, пов'язаних із веб-контентом та файлами. Цей інструмент входить до пакетів Transformation і Unlimited, а також доступний як додаток до пакету Business. Інтерфейс Zscaler інтуїтивно зрозумілий та зручний для користувача. Як інструмент інтернет-безпеки, Zscaler Internet Access також пропонує додаткові функції, такі як запобігання витоку даних (DLP), шлюз для захисту веб-доступу та посередник безпеки хмарного доступу (CASB). Зміни конфігурації та політики можуть бути миттєво впроваджені, що гарантує синхронну роботу всієї мережі. Крім того, автоматизація тестів безпеки та пов'язаних завдань знижує навантаження на адміністраторів.

РОЗДІЛ 3 АНАЛІЗ РІВНЯ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ

Для того щоб детально вивчити та проаналізувати рівень захищеності інформації в мережі треба побувати в ролі зловмисника та знати основні способи та методи для проведення розвідки, збору інформації та аналізу.

3.1 Тест на проникнення, застосування інструментів Kali Linux, Nmap, Wireshark , MegaPing

Сканування мереж — це техніка, яка використовується в комп'ютерній безпеці для збору інформації про цільову мережу. Інформація, зібрана під час сканування, включає відомості про хости, підключені до мережі, відкриті порти, служби, що працюють на цих портах, і використовувані операційні системи. Метою сканування є виявлення потенційних вразливостей у мережі, що дозволяє зловмиснику визначити найкращий спосіб проникнення в мережу. Існує кілька типів сканування мережі, включаючи сканування портів, сканування ping, сканування відбитків ОС, сканування вразливостей тощо. Інструменти, які використовуються для сканування мережі, включають Nmap, Nessus, OpenVAS тощо. Сканування зазвичай вважається етапом перед нападом і використовується для збору інформації та підготовки до потенційної атаки. Сканування мереж — це процес активного дослідження комп'ютерних мереж для збору інформації про мережеві системи та об'єкти, до яких вони належать. Метою сканування мережі є ідентифікація пристроїв, підключених до мережі, їхніх IP-адрес, відкритих портів і запущених на них служб.

Ця інформація має вирішальне значення для розуміння стану безпеки мережі, виявлення вразливих систем і потенційних цілей для атак. Існують різні типи сканування мережі, наприклад сканування портів, сканування ping і сканування вразливостей. Сканування портів використовується для визначення відкритих портів і служб у системі, тоді як сканування ping використовується для визначення наявності активних систем у мережі. Сканування вразливостей, з іншого боку, перевіряє відомі вразливості в системах і програмах і повідомляє про потенційні

ризика безпеці. Сканування мереж є важливим кроком у процесі тестування на проникнення, і його часто виконують фахівці з безпеки, щоб оцінити безпеку мережі та виявити потенційні слабкі місця. Однак його також можуть використовувати зловмисники для збору інформації для своїх атак і компрометації систем.

Використання методів створення пакетів UDP і TCP hping3

Hping3 — це інструмент безпеки мережі, який використовується для надсилання та аналізу мережевих пакетів. Його можна використовувати для перевірки правил брандмауера, сканування мережі та надсилання різних типів мережевих пакетів. Hping3 здатний надсилати пакети TCP, UDP і ICMP і може використовуватися для перевірки безпеки цільової системи. Hping3 широко використовується фахівцями з безпеки та вважається універсальним і ефективним інструментом для виконання різних типів мережевого тестування та аналізу.

Створення пакетів стосується процесу створення програмного пакета, який є попередньо налаштованим архівним файлом, який містить усі необхідні файли, бібліотеки та залежності для програмного додатку. Пакет створено для полегшення розповсюдження, встановлення та керування програмним забезпеченням. Процес створення пакета включає такі завдання, як створення пакета з вихідного коду, створення маніфесту пакета та тестування пакета. Метою створення пакетів є полегшення встановлення та використання програмного забезпечення для користувачів, а також спрощення керування програмним забезпеченням для системних адміністраторів.

Входимо у Kali Linux і запускаємо термінал. Використовуйте hping3-h для відображення всіх команд. Ми зосередимося на кількох із них.

Hping3 -c 3 <Target IP address>

3 packets transmitted, 3 packet received, 0% packet loss

внизу вихідних даних було надіслано та отримано 3 пакети. Ви повинні отримати цю відповідь. -c означає кількість пакетів. Означає, що ми хочемо надіслати лише три пакети на цільову машину. Далі ми надішлемо сканування прапора SYN із діапазоном портів.

hping3 -scan 1-3000 -S <Target IP address>

```
Scanning 10.0.2.15 (10.0.2.15), port 1-3000
3000 ports to scan, use -V to see all the replies
+---+-----+-----+-----+-----+-----+
|port| serv name | flags |ttl| id  | win | len |
+---+-----+-----+-----+-----+
135 epmap      : .S..A... 128 62018 65392 46
139 netbios-ssn: .S..A... 128 63042 8192 46
445 microsoft-d: .S..A... 128 52291 65392 46
All replies received. Done.
Not responding ports:
```

Рисунок 3.1 – Сканування портів

-scan параметр визначає діапазон портів для сканування. -S представляє прапор SYN. Результат показує відкриті порти на цільовій машині, тобто Windows 10.

Знову запускаємо Wireshark на машині Windows і залишаємо його працювати. Щоб надіслати запит TCP SYN на цільову машину, вводимо:

hping3 -S <Target IP address> -p 80 -c 5

Це передасть запит на 5 пакетів на комп'ютер жертви через порт 80. -S виконає запит TCP SYN на цільовому пристрої, р передаватиме трафік, через який призначений порт, і -c є кількістю пакетів, надісланих на цільову машину. Переходимо на цільову машину (Windows) і спостерігаємо за TCP-пакетами, зібраними в Wireshark. Потім зупиняємо захоплення пакетів і починаємо нове захоплення знову. Залишаємо Wireshark запущеним.

hping3 <Target IP address> --flood

Надсилаємо -flood пакети якомога швидше, не піклуючись про відображення вхідних відповідей. Через кілька секунд зупиніть захоплення пакетів у Wireshark у Windows. Ви помітите TCP-флуд з машини зловмисника. Примітка. Якщо ви хочете перевірити потік пакетів TCP і провести зворотне проектування, переконайтеся, що ви розумієте більше, ніж сумнозвісне «тристороннє рукостискання».

Ідентифікація операційної системи (ОС), яка використовується на цільовому хості

Ідентифікація операційної системи (ОС), яка використовується на цільовому хості, — це процес визначення конкретного типу операційної системи, встановленої на цільовій комп'ютерній системі. Цю інформацію можна отримати за допомогою різних методів, включаючи засоби сканування мережі, такі як Nmap, або шляхом вивчення відповіді цільової системи на різні типи запитів. Знання ОС, яка використовується на цільовому хості, важливо для виконання різних завдань, таких як оцінка вразливості, тестування на проникнення та розробка експлойтів. ОС, яка використовується на цільовому хості, може надавати інформацію про потенційні вразливості безпеки та потенційні вектори атак, які можна використати в процесі компрометації цільової системи.

Існує два типи техніки захоплення банерів: активна і пасивна. Захоплення банерів або відбитки ОС — це метод визначення ОС, що працює на віддаленій системі.

Операційна система	Термін життя (TTL)	Розмір вікна TCP
Linux (ядро 2.4 і 2.6)	64	5840
FreeBSD	64	65535
OpenBSD	64	65535
Google налаштував Linux	64	5720
Windows XP	128	65535
Windows 7, Vista і Server 2008	128	8192
Маршрутизатор Cisco IOS 12.4	255	4128

Рисунок 3.2 – Порівняння ОС

Використання Wireshark для виявлення TTL

— відкриваємо Wireshark на комп'ютері з Windows 10, вибираємо правильний інтерфейс і починаємо зйомку. (Інтерфейс може відрізнятися від вашого середовища).

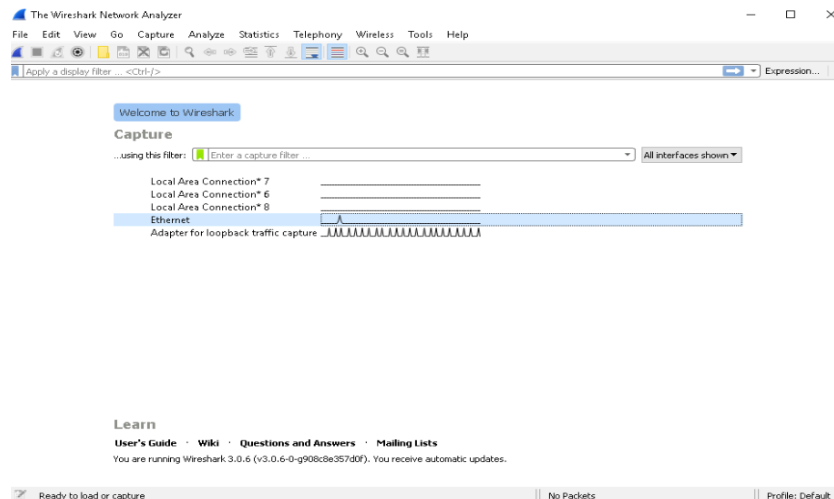


Рисунок 3.3 – Програмне забезпечення Wireshark

— переходимо на комп'ютер Ubuntu і починаємо перевіряти комп'ютер з Windows 10.

```
ping -c 10 <Target IP Address[Windows 10]>

msfadmin@metasploitable:~$ ping -c 10 10.0.2.37
PING 10.0.2.37 (10.0.2.37) 56(84) bytes of data:
64 bytes from 10.0.2.37: icmp_seq=1 ttl=128 time=0.532 ms
64 bytes from 10.0.2.37: icmp_seq=2 ttl=128 time=0.447 ms
64 bytes from 10.0.2.37: icmp_seq=3 ttl=128 time=0.438 ms
64 bytes from 10.0.2.37: icmp_seq=4 ttl=128 time=0.453 ms
64 bytes from 10.0.2.37: icmp_seq=5 ttl=128 time=0.479 ms
64 bytes from 10.0.2.37: icmp_seq=6 ttl=128 time=0.504 ms
64 bytes from 10.0.2.37: icmp_seq=7 ttl=128 time=0.430 ms
64 bytes from 10.0.2.37: icmp_seq=8 ttl=128 time=0.502 ms
64 bytes from 10.0.2.37: icmp_seq=9 ttl=128 time=0.478 ms
64 bytes from 10.0.2.37: icmp_seq=10 ttl=128 time=0.748 ms

--- 10.0.2.37 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8999ms
rtt min/avg/max/mdev = 0.430/0.501/0.748/0.088 ms
msfadmin@metasploitable:~$ _
```

Рисунок 3.4 – Перевірка зв'язку між комп'ютерами

— повертаємось до Wireshark і перевіряємо протокол ICMP, вибравши захоплений кадр пакета; Розгорніть вузол «Версія Інтернет-протоколу» в деталях пакета, ви побачите TTL. Значення TTL, записане як 64 означає, що запит ICMP надійшов із машини на базі Linux.

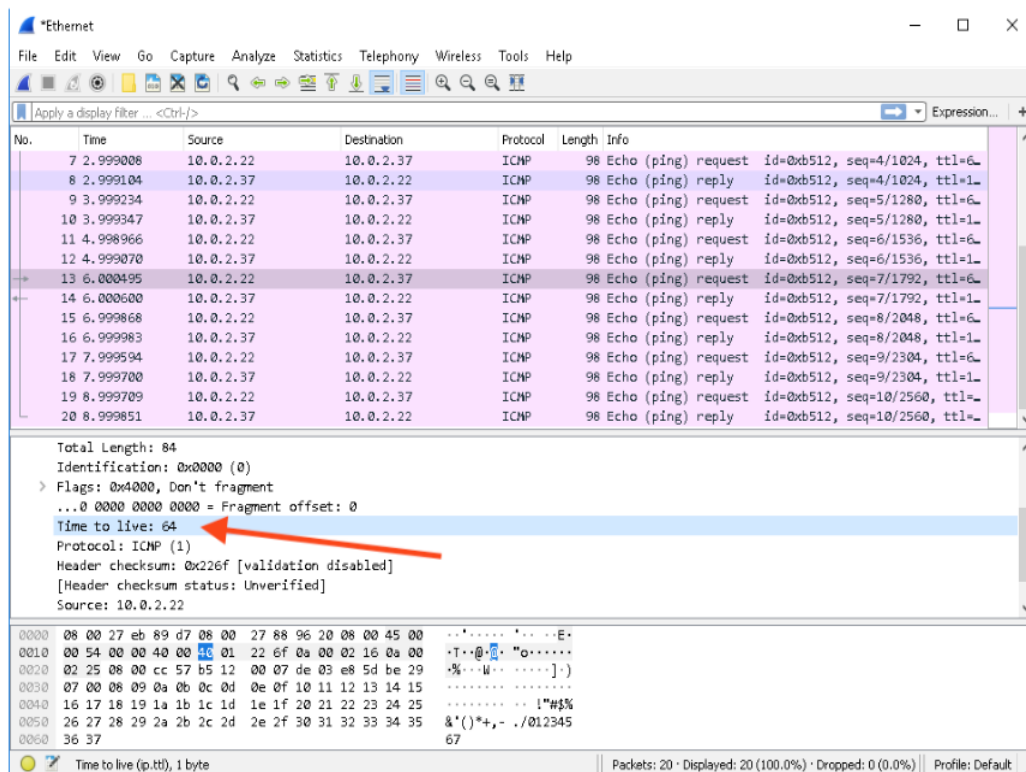


Рисунок 3.5 – Перевірка протоколу ICMP в Wireshark

— оновлюємо Wireshark, запустивши інше захоплення, і переходимо до Windows 7. Повторюємо той самий процес, але з машиною Windows 7. Відкриваємо підказку або Powershell і виконуємо перевірку ping до машини з Windows 10, на якій запущено Wireshark.

ping <Target IP Address>

— Повертаємось до Wireshark на машині з Windows 10 і знову перевіряємо ту саму інформацію про TTL. Значення TTL, записане як 128 означає, що запит ICMP надійшов із комп'ютера під керуванням Windows.

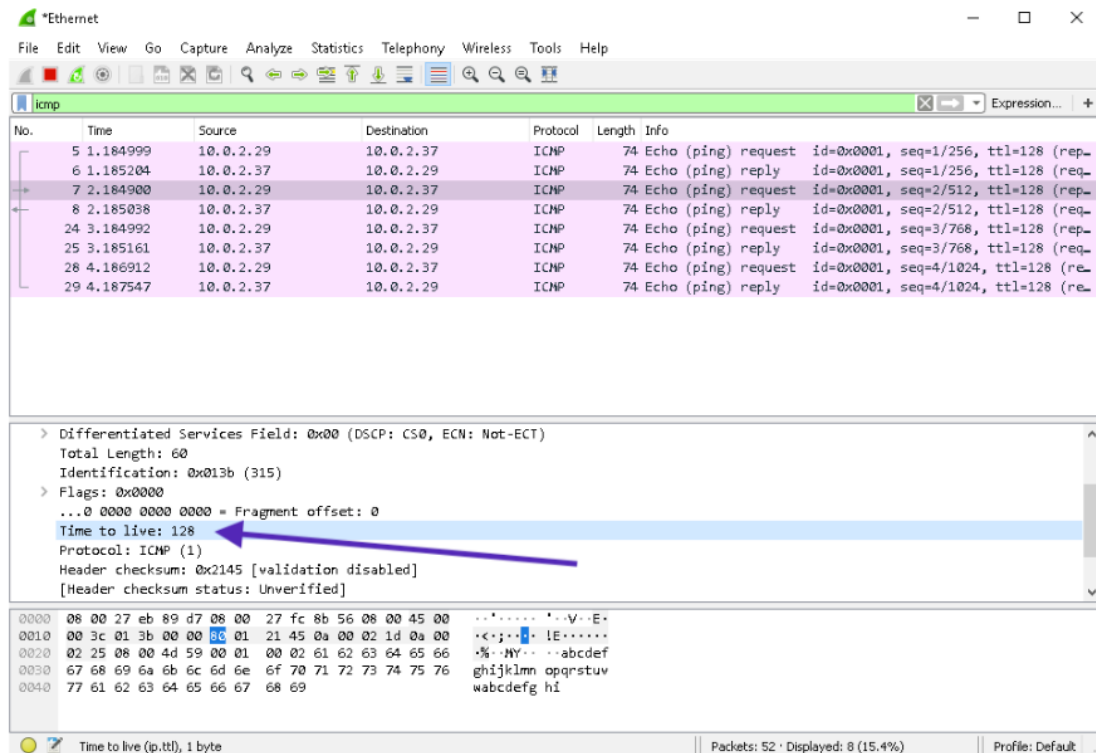


Рисунок 3.6 – Перевірка протоколу ICMP в Wireshark

Основне усунення несправностей мережі за допомогою MegaPing (Windows)

MegaPing — це мережевий інструментарій, який дозволяє користувачам виконувати діагностичні тести мережі, зокрема ping, traceroute, Whois, nslookup тощо. Він створений як універсальний мережевий інструмент для операційних систем Windows, що дозволяє користувачам швидко діагностувати та усувати проблеми з мережею. MegaPing можна використовувати для моніторингу доступності кількох мережевих пристроїв, діагностики проблем з підключенням і виявлення проблем із затримкою мережі. Крім того, він надає розширені функції, такі як спеціальні зонди, регульовані тайм-аути та настроювані параметри відображення.

Це програмне забезпечення дуже просте у використанні. Щоб розпочати сканування, натисніть IP-сканер на лівій панелі.

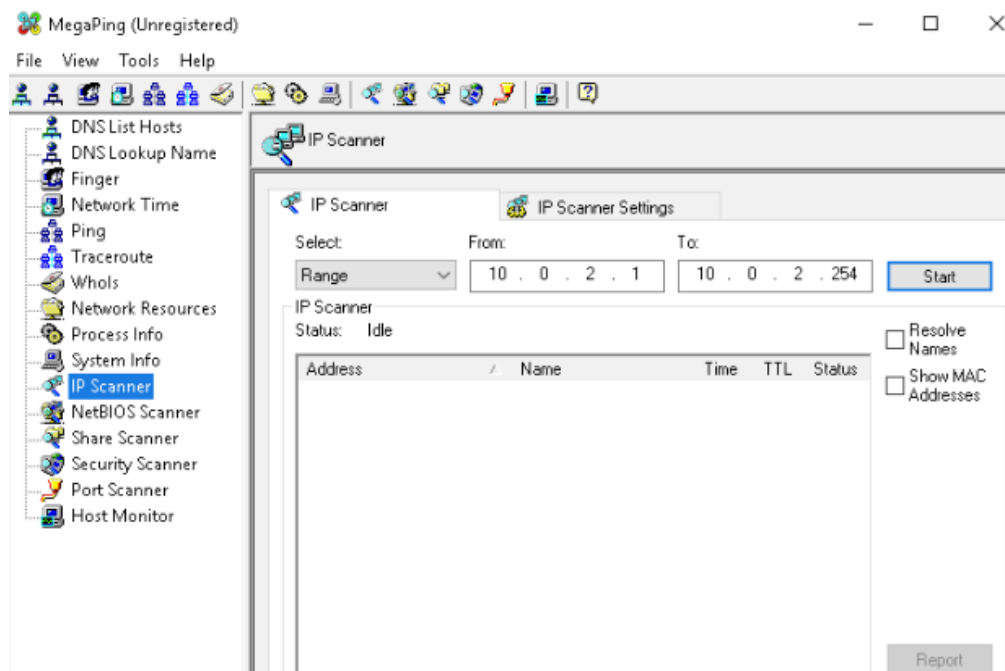


Рисунок 3.7 – Програмне забезпечення MegaPing

Вказуємо діапазон IP-адрес мережевої лабораторії та натискаємо «Пуск». Звертаємо увагу на прапорець праворуч, ви можете переглянути MAC-адреси зібраних хостів. MegaPing перераховує всі IP-адреси у вказаному цільовому діапазоні з їхнім TTL статусом (мертвий чи живий) і статистикою.

Правою кнопкою миші IP-адресу вибираємо Traceroute. Ця дія виконає Traceroute, відображаючи кількість стрибків, зроблених головною машиною для досягнення мети. Виконуємо сканування портів на цільовому хості.

Ця дія перерахує всі порти, пов'язані з метою, разом із типом порту, ключовим словом, ризиком і описом, як показано на наступному знімку екрана:

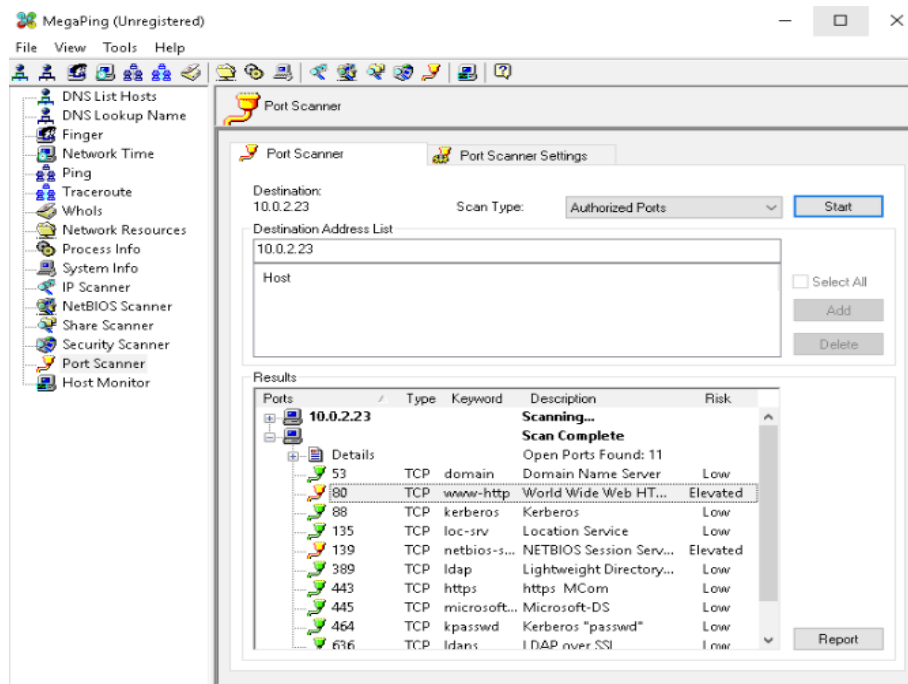


Рисунок 3.8 – Відображення портів в MegaPin

Сканування за допомогою Nmap

У постійно мінливому ландшафті кібербезпеки важливо мати у своєму розпорядженні інструменти, які допоможуть вам оцінити безпеку вашої мережі та виявити потенційні вразливості. Зокрема, одним з таких інструментів є Nmap. Цей потужний інструмент для сканування мережі, який широко використовується як фахівцями з безпеки, так і хакерами, дозволяє виявляти хости в мережі, а також визначати відкриті порти. Крім того, Nmap забезпечує можливість збору детальної інформації про системи, які підключені до вашої мережі.

Nmap, скорочено від Network Mapper, є безкоштовним інструментом сканування мережі з відкритим вихідним кодом, який був розроблений Гордоном Лайоном у 1997 році. Відтоді він став одним із найпопулярніших і широко використовуваних інструментів для мережевої розвідки та аудиту безпеки. Більш того, Nmap доступний для різних операційних систем, таких як Windows, Linux і Mac OS X, що робить його доступним для широкого кола користувачів.

Nmap використовує необроблені IP-пакети, щоб визначити, які хости доступні в мережі, які послуги (назва і версія програми) ці хости пропонують, а також які операційні системи (і версії ОС) вони використовують. Крім того, програма може ідентифікувати типи пакетних фільтрів чи брандмауерів, які

використовуються, а також визначити десятки інших характеристик. Зрештою, Nmap була розроблена для швидкого сканування великих мереж, проте вона однаково добре працює і з окремими хостами.

Вихідні дані Nmap - це список просканиваних цілей з додатковою інформацією по кожній з них залежно від заданих опцій. Ключовою інформацією є "таблиця важливих портів". Ця таблиця містить номер порту, протокол, ім'я служби та стан. Стан може мати значення open (відкритий), filtered (фільтрується), closed (закритий) або unfiltered (не фільтрується). Відкритий означає, що додаток на цільовій машині готовий для встановлення з'єднання/прийняття пакетів на цей порт. Фільтрується означає, що брандмауер, мережевий фільтр, або якась інша перешкода в мережі блокує порт, і Nmap не може встановити, відкритий цей порт чи закритий. Закриті порти не пов'язані з жодним додатком, але можуть бути відкриті в будь-який момент. Порти розцінюються як не фільтровані, коли вони відповідають на запити Nmap, але Nmap не може визначити, відкриті вони чи закриті. Nmap видає комбінації відкритий|фільтрується і закритий|фільтрується, коли не може визначити, який із цих двох станів описує порт. Ця таблиця також може надавати деталі про версію програмного забезпечення, якщо це було запитано. Коли здійснюється сканування за IP протоколом (-sO), Nmap надає інформацію про підтримувані протоколи, а не про відкриті порти.

Додатково до таблиці важливих портів Nmap може надавати подальшу інформацію про цілі: перетворені DNS імена, припущення про використовувану операційну систему, типи пристроїв і MAC-адреси.

Типове сканування з використанням Nmap показано нижче. Єдині аргументи, використані в цьому прикладі, - це -A, для визначення версії ОС, сканування за допомогою сценаріїв і трасування; -T4 для більш швидкого виконання; потім два цільових хости.

```
# nmap -A -T4 scanme.nmap.org playground

Starting Nmap ( https://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http      Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11

Interesting ports on playground.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
135/tcp    open  msrpc     Microsoft Windows RPC
139/tcp    open  netbios-ssn
389/tcp    open  ldap?
445/tcp    open  microsoft-ds   Microsoft Windows XP microsoft-ds
1002/tcp   open  windows-icfw?
1025/tcp   open  msrpc     Microsoft Windows RPC
1720/tcp   open  H.323/Q.931   ComPTek AquaGateKeeper
5800/tcp   open  vnc-http     RealVNC 4.0 (Resolution 400x250; VNC port: 5900)
5900/tcp   open  vnc         VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

Рисунок 3.9 – Сканування за допомогою Nmap

Скануємо всю підмережу.

Відкриваємо вікно терміналу та введіть nmap-h список усіх доступних команд.

```
nmap -O <IP Range>
```

Параметр `-o` пов'язаний із виявленням операційної системи.

Для визначення діапазону IP можна використовувати два способи:

Символ підстановки: `nmap -O 10.0.2.*`

Позначення підмережі: `nmap -O 10.0.2.1/24`

Рисунок 3.10 – Інформація про Nmap

Запускаємо це сканування та перевіряємо результати. Nmap сканує всю мережу та відображає інформацію для всіх хостів разом із відкритими портами, типом пристрою, деталями ОС.

Виберіть один хост, який ви просканували

```
nmap --packet-trace 10.0.2.23
```

Видаючи `--packet-trace` команду, Nmap надсилає кілька пакетів на призначену машину та отримує пакети у відповідь на надіслані пакети. Він друкує підсумок кожного пакета, який надсилає та отримує.

Наведені нижче результати показують пакети, надіслані від хоста до цільового, та пакети, отримані від цільового хосту.

```
...
SENT (4.1431s) TCP 10.0.2.15:35962 > 10.0.2.23:3005 S ttl=43 id=22968 iplen=44 seq=1965204224 win=1024 <mss 1460>
SENT (4.1433s) TCP 10.0.2.15:35962 > 10.0.2.23:4000 S ttl=39 id=51710 iplen=44 seq=1965204224 win=1024 <mss 1460>
SENT (4.1434s) TCP 10.0.2.15:35962 > 10.0.2.23:1503 S ttl=53 id=146 iplen=44 seq=1965204224 win=1024 <mss 1460>
SENT (4.1435s) TCP 10.0.2.15:35962 > 10.0.2.23:1761 S ttl=56 id=27951 iplen=44 seq=1965204224 win=1024 <mss 1460>
```

Рисунок 3.11 – Команда `--packet-trace` в Nmap

Зверніть увагу, що внизу вихідних даних також показано відкриті порти TCP:

PORT	STATE	SERVICE
53/tcp	open	domain
80/tcp	open	http
88/tcp	open	kerberos-sec
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
443/tcp	open	https
445/tcp	open	microsoft-ds
...		

Рисунок 3.12 – Відкриті порти TCP

Ідентифікуємо служби за допомогою TCP Null Scan

- -sN: нульове сканування TCP.
- -A: вмикає визначення ОС, визначення версій, сканування сценаріїв і traceroute
- -T4: Час: (4) Агресивний режим прискорює сканування, припускаючи, що ви перебуваєте в досить швидкій і надійній мережі.

Виконуючи цю команду, Nmap надсилає TCP-пакети, у яких не встановлено жоден із позначок TCP. Якщо сканування повертає пакет RST, це означає, що порт закрито; Якщо нічого не повертається, порт або відфільтрований, або відкритий.

```
...
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
...
```

Рисунок 3.13 – Частина результату сканування, виконаного на Metasploitable Linux

Як показано вище, ми можемо побачити частину результату сканування, виконаного на Metasploitable Linux. Пізніше ми зможемо перевірити версії та тип

служб, що працюють на відкритих портах. Цей тип інформації дуже цінний, оскільки ми можемо шукати вразливості, недоліки тощо.

Nmap постачається з різними вбудованими сценаріями, які можна використовувати під час процесу сканування, щоб знайти відкриті порти та служби, що працюють на портах. Підсумок сканувань, які будуть виконані:

1. TCP Connect Scan використовує звичайне TCP-з'єднання, щоб визначити, чи доступний порт. Це сканування є найпростішим із сканування TCP. Системний виклик connect(), наданий вашою ОС, використовується для з'єднання з кожним цікавим портом на машині. Якщо порт прослуховує, connect() буде успішним, інакше порт недоступний. Однією з переваг цієї техніки є те, що вам не потрібні особливі привілеї.

```
nmap -sT -T3 -A <Target IP address>
```

2. Xmas Scan передбачає надсилання сегментів TCP із усіма прапорами, надісланими в заголовку пакета, генеруючи пакети, які є незаконними згідно з RFC. Xmas Scan надсилає кадр TCP на віддалений пристрій із установленими прапорцями PSH, URG і FIN. FIN сканує лише за допомогою ОС TCP/IP, розробленої відповідно до RFC 793. Поточна версія MS Windows не підтримується.

```
nmap -sX -T4 <Target IP adress>
```

3. Сканування UDP передбачає надсилання загального UDP-пакета до цільового пристрою. Сканування UDP виконується для пошуку будь-яких портів UDP на цільовій машині. Якщо є, щоб визначити їх стан (Відкрито/Закрито).

```
nmap -sU -T5 <Target IP adress>
```

4. Сканування прапора ACK передбачає надсилання пакета зонда ACK із випадковим порядковим номером. Сканування ACK ніколи не знаходить відкритий порт. Він забезпечує лише «відфільтроване» або «нефільтроване» розташування, оскільки ніколи не підключається до програми для підтвердження «відкритого» стану. Це сканування ініціює сканування ACK і відображає розташування портів.

```
nmap -sA -v -T4 <Target IP adress>
```

5. Сканування IDLE передбачає надсилання підроблених пакетів до цілі. Сканування в режимі очікування — це техніка, яка використовується хакерами для

сканування портів, приховуючи свою IP-адресу. Це досягається шляхом використання неактивного хоста (зомбі) між зловмисником і цільовою системою, який використовується для надсилання пробних пакетів до цілі. Відповідь від цілі надсилається назад до зловмисника через той самий зомбі-хост, створюючи враження, ніби тестові пакети були надіслані з зомбі-хосту, а не з IP-адреси зловмисника. Це дозволяє зловмиснику збирати інформацію про цільову систему, не будучи виявленим. У цьому прикладі зомбі буде машиною Windows Server 2012 і цільовою машиною Windows 10, яка використовує номер порту 80 (або будь-який порт, який ви хочете перевірити).

```
nmap -Pn -p 80 -sI <IP address of the zombie> <Target IP address>
```

```
Idle scan using zombie 10.0.2.37 (10.0.2.37:80); Class: Incremental
Nmap scan report for 10.0.2.23
Host is up (0.0069s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 22:44:11:55:66:77 Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

Рисунок 3.14. – Результат виконання команди

3.2 Інструменти що виявляють невидимі загрози, які можуть означати кібератаку, Zscaler Deception, FortiDeceptor, CyberTrap, Cisco Stealthwatch, Illusive Shadow.

У зв'язку зі стрімким зростанням та модифікацією хакерських атак, актуальним питанням стає дослідження різних засобів захисту, які б дозволяли аналізувати поведінку зловмисника в мережі. Відомі методи захисту мають свої недоліки і в більшості випадків не дозволяють проаналізувати дії нападника в ході реалізації атаки. Для вирішення цих задач розробляються нові технології захисту, відомі як Deception Technology, які дозволять зменшити завантаженість системи (кількість подій безпеки) і допомагають аналізувати дії зловмисника в режимі реального часу. Deception Technology як технологія яка не тільки долає основний недолік стандартних засобів захисту, а саме велику кількість згенерованих подій безпеки, які потрібно обробляти, зберігати та реагувати на них, а й дозволяє досліджувати й аналізувати дії зловмисників.

Zscaler Deception - це просте, швидке та ефективне рішення для цільового виявлення загроз, побудоване на архітектурі Zscaler Zero Trust. Deception використовує передові приманки для виявлення та знешкодження складних загроз, які постійно обходять традиційні засоби захисту, такі як сучасні постійні загрози (APT), експлойти, розвідка, латеральний рух, активні каталоги, ланцюжки поставок, програми-вимагачі, керовані людиною, системи диспетчерського контролю та збору даних (SCADA) та атаки на промислові системи управління (ICS). Як невід'ємна частина Zscaler Zero Trust Exchange, Deception інтегрується з Zero Trust, відстежуючи повну послідовність атаки і ініціюючи автоматизовані дії реагування на платформі Zscaler. Zscaler Deception розгортає реалістичні приманки у вашому середовищі, щоб заманювати, виявляти та перехоплювати активних зловмисників. Коли скомпрометований користувач взаємодіє з приманкою, ваша команда отримує негайне сповіщення — зловмисники ніколи не дізнаються, що їх спіймали, доки не стає надто пізно.

Зловмисники стають винятковими у використанні зростаючих поверхонь атак організацій. Просунуті атаки обходять існуючий захист. Виявляти та локалізувати їх складно, оскільки:

- Розширені атаки є прихованими, і 91% атак не генерують сповіщення безпеки.
- Просунуті атаки здійснюються людьми, і 68% атак не використовують зловмисне програмне забезпечення.
- Команди безпеки мають надто багато подій для розслідування, оскільки 45% сповіщень є помилковими.

Обман використовує методи активного захисту, щоб зробити вашу мережу ворожим середовищем для зловмисників. Він покриває ваше середовище приманками для всіх ваших ІТ-артефактів. Приманки роблять ваше оточення непередбачуваним і руйнують підручники зловмисників. Приманки заманюють зловмисників і виявляють передові атаки без операційних витрат або помилкових спрацьовувань. Обман є надійним доповненням до виявлення загроз вашої

організації та стратегії Zero Trust. Це найпростіший спосіб додати потужний рівень високоточного виявлення загроз.

Ключові особливості та переваги Deception включають:

- Простота розгортання: інтеграція з Zscaler Zero Trust Exchange забезпечує безпроблемне розгортання. Deception доставляється в хмарі та масштабується, і вимагає мінімальних локальних обчислень. Він не потребує додаткового оновлення обладнання.

- Всебічне покриття: забезпечує виявлення загроз для вашого периметра, додатків, кінцевих точок, активних каталогів, хмари та середовищ операційних технологій (OT) або Інтернету речей (IoT).

- Велика кількість вбудованих приманок: легко налаштовувати та керувати приманками, які залучають кмітливих противників.

- Знищення розширених загроз: виявляє та зупиняє зловмисників у вашій інфраструктурі безпеки, включаючи малопомітні шляхи, такі як DC-DC і внутрішній трафік-DC.

- Низький рівень хибних спрацьовувань: не існує законного бізнес-трафіку для приманок, тому будь-яка взаємодія з ними є миттєвим високодостовірним сигналом про поточний злом, який попереджає вашу команду безпеки про такі загрози, як програми-вимагачі, атаки на ланцюги поставок і APT.

- Поінформованість про бізнес-ризик: чітко узгоджує засоби безпеки з ділянками з поточними бізнес-ризиками.

- Оркестроване реагування: організовує складні сценарії за допомогою високоточних сповіщень. Виконує точні дії, щоб зупинити активні атаки, керуючись сповіщеннями високої достовірності.

- Активний захист із структурою MITER ATT&CK: надає 99% можливостей, охоплених MITER Engage.

Щоб розмістити приманки у вашій мережі, Deception дозволяє налаштувати з'єднувачі Decoy і підключити їх до порталу адміністратора Zscaler Deception. Ви можете налаштувати віртуальні локальні мережі (VLAN) у своєму середовищі для розгортання мережевих приманок. Якщо ви розгорнули Zscaler Private Access

(ZPA) для доступу до мережі з нульовою довірою, ви можете інтегрувати Deception із ZPA для розгортання приманок для мережі з нульовою довірою, не встановлюючи жодних додаткових компонентів мережі та не вносячи жодних змін у конфігурації мережі.

Обман дозволяє налаштовувати та розгорнути приманки, щоб перешкоджати активним атакам, створювати підроблені шляхи атак і отримувати високоточні дані про загрози. Deception надає численні вбудовані приманки по всьому ланцюжку вбивств, які імітують виробничі активи. Ви можете налаштувати та розгорнути мережеві приманки, приманки Threat Intelligence (TI), приманки Active Directory (AD), приманки кінцевих точок і хмарні приманки. Крім того, ви можете використовувати великі набори даних у Miragemaker, щоб зробити приманки більш реалістичними та масштабованими.

Коли зломисник проникає у вашу мережу та взаємодіє з приманками, Deception виявляє загрози, збирає інформацію про дії та наміри зломисника та генерує високоякісні сповіщення в реальному часі.

Коли сповіщення з'являються на порталі адміністратора Deception, Deception фіксує дані розвідки про загрози та розвідувальну діяльність у режимі реального часу. ThreatParse проводить реконструкцію атак природною мовою, узагальнює інформацію журналу та перекладає її простою англійською мовою, щоб допомогти центру безпеки (SOC) і аналітикам зрозуміти, чого намагається досягти зломисник. SOC та аналітики можуть співвідносити ці дані, щоб генерувати дані про загрози та вживати необхідних заходів, щоб зупинити бічний рух.

Базуючись на високоточних даних, Deception дає змогу оркеструвати (автоматизувати) і створювати правила для вжиття негайних дій, коли виявляється, що події містять загрози.

Коли намічені цілі зломисника виявлені, Deception розгортає додаткові приманки для перевірки виправлення.

FortiDeceptor, частина платформи Fortinet SecOps, виявляє та реагує на атаки в мережі, такі як використання вкрадених облікових даних, сторонній рух, "людина посередині" та програми-вимагачі. Додавання FortiDeceptor як частини вашої

стратегії кібербезпеки допомагає змінити ваш захист із реактивного на проактивний із виявленням вторгнень із контекстним інтелектом.

FortiDeceptor спонукає зловмисників виявити себе на ранній стадії розвідки, використовуючи широкий спектр обманних ресурсів, розподілених у вашому середовищі. Платформа генерує високоточні сповіщення на основі взаємодії зловмисників і зловмисного програмного забезпечення в режимі реального часу, забезпечуючи аналіз активності атак і ізоляцію атак. Це допомагає полегшити навантаження на команди SOC, завалені хибнопозитивними сповіщеннями. FortiDeceptor пропонує гнучкі варіанти розгортання: SaaS (хмарне розміщення), локальне (HW/VM) і публічне хмарне середовище (AWS, Azure, GCP).

Зловмисники неодноразово доводили, що вони можуть використовувати прогалини в безпеці для проникнення у вашу мережу, а потім пересуватися непоміченими протягом тривалого часу. Більшість організацій не можуть виявити або відреагувати на загрози, які отримали доступ достатньо швидко, щоб запобігти шкоді. За допомогою FortiDeceptor-as-a-Service ви можете використовувати передові технології обману щоб змусити зловмисників взаємодіяти з підробленими активами, даними та додатками. Це дозволяє виявити атаку та зупинити її на ранній стадії циклу атаки. Послуга забезпечує високу точність нуль хибнопозитивних спрацьовувань завдяки багатим аналітичним даним про загрози та практичним рекомендаціям. FortiDeceptor-as-a-Service - це рішення без агентів, яке не впливає на стабільність, продуктивність і безперервність роботи мережі.

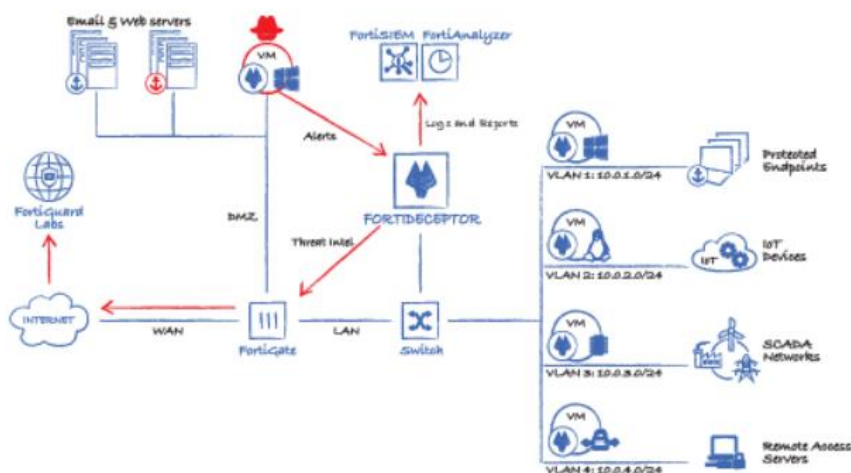


Рисунок 3.15 – FortiDeceptor

FortiDeceptor створює мережу віртуальних машин Decoy, щоб заманювати зловмисників і контролювати їхню діяльність у мережі. Коли зловмисники атакують віртуальні машини Decoy, їхні дії аналізуються для захисту мережі.

Особливості та переваги:

- Видимість і прискорене реагування. Інтегрується з Fortinet Security Fabric і сторонніми засобами контролю безпеки (SIEM, SOAR, EDR, пісочниця),
- Виявлення інсайдерської загрози. Зменшує час перебування та помилкові спрацьовування, виявляє ранню розвідку та бічний рух для неправильного спрямування атак,
- Криміналістика та розвідка загроз. Фіксує та аналізує дії атак у реальному часі, надає детальну криміналістику, збирає IOC та TTP,
- Карантинні/некарантинні атаки. Заражені кінцеві точки можна вивести на карантин із робочої мережі,
- Оптимізовано для мереж OT/IOT. Велика кількість приманок включає системи SCADA, датчики Інтернету речей, а також ви можете завантажити власні приманки,
- Просте розгортання та обслуговування. Приманки для збігу активів розгортаються автоматично, не впливаючи на стабільність і продуктивність



Рисунок 3.16 – Варіанти використання FortiDeceptor

Вимоги до операцій безпеки, як-от виявлення загроз і реагування на них, з кожним роком стають дедалі складнішими. Відповідно до звіту про економічну

перевірку Enterprise Strategy Group TechTarget, для виявлення загроз може знадобитися в середньому 168 годин або більше, тоді як багато загроз ніколи не виявляються. Тому CISO повинні розглянути технологію обману для покращення виявлення загроз і реагування на них. Сучасна технологія обману, як-от FortiDeceptor, поєднує історичну цінність технології обману з простотою використання, автоматизацією та ефективним інтелектом, створюючи активний захист. Ці переваги особливо важливі для організацій з обмеженим персоналом і навичками безпеки, а також для тих, хто об'єднує IT та OT.

CyberTrap — це передова високоінтерактивна технологія обману, яка дозволяє аналізувати та контролювати порушення безпеки в реальному часі. CyberTrap стежить за цілеспрямованими атаками на вашу критично важливу інфраструктуру та інформує вашу службу безпеки про будь-які успішні зломи. Щойно зловмисники потрапляють у пастку, за ними здійснюється дуже детальний і всебічний моніторинг. CyberTrap допоможе вам дізнатися, які методи та інструменти використовують зловмисники та чого вони прагнуть, а не просто блокувати те, що вони роблять. У той же час ваші співробітники служби безпеки повністю контролюють CyberTrap - зловмисників можна видалити або розмістити нові приманки, щоб дізнатися ще більше про їхні дії. Крім того, функція «атрибуції» допоможе вам визначити інфраструктуру та походження зловмисників.

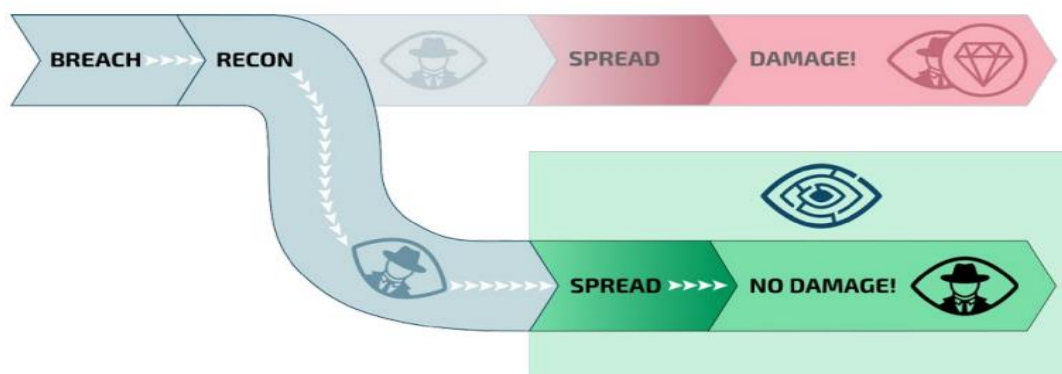


Рисунок 3.17 – Робота CyberTrap

CyberTrap працює поза брандмауером і діє як додатковий рівень захисту та розширення існуючих систем безпеки. CyberTrap — це новий революційний крок у сфері кібербезпеки. Замість того, щоб блокувати зловмисників, ми вводимо їх у в

обмежене, контрольоване середовище для відстеження їх усередині мережі для збору розвідувальних даних. У нашому сценарії зловмисник не тільки покаже нам діри в паркані, а й розповість, хто він і що шукає.

Cisco StealthWatch - по суті це засіб забезпечення ІБ в мережі, який заснований на збиранні телеметричних даних з різних пристроїв, тобто не тільки з МСЕ, що стоять на периметрі, а також з інфраструктурних пристроїв, як-от маршрутизатори, комутатори, сервери з віртуальними машинами та навіть із користувацьких пристроїв (не важливо, чи під'єднані вони зсередини корпоративної мережі, чи перебувають за її межами).

Оскільки основним протоколом збору даних про телеметрію в рішенні Cisco StealthWatch є широковідомий і популярний NetFlow/IPFIX, це дає змогу 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.

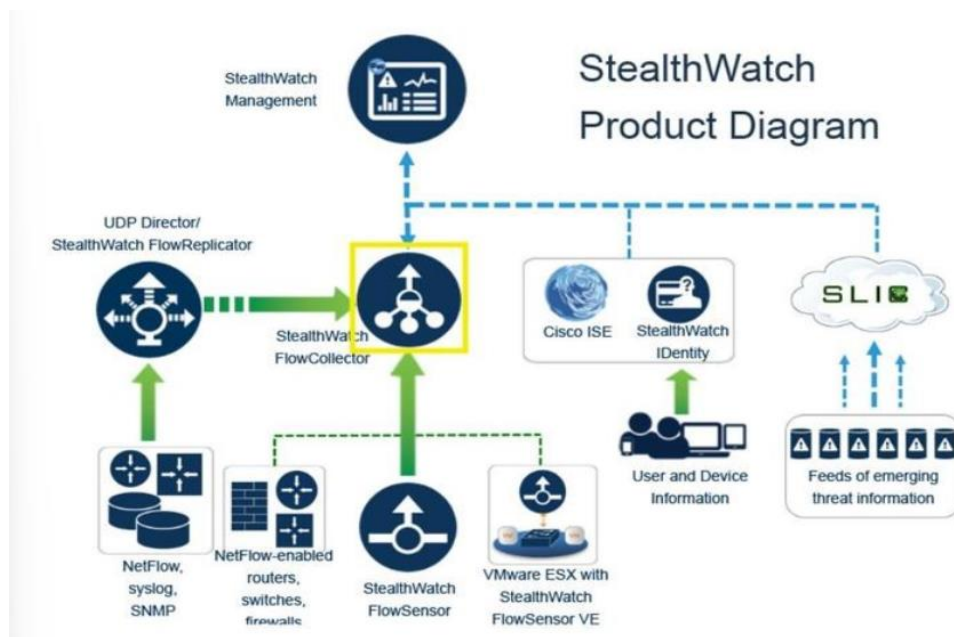


Рисунок 3.18 – Cisco StealthWatch

Причому Cisco StealthWatch не просто збирає ці дані (тобто є колектором цих даних), він уміє їх дедуплікувати, збагачувати дані телеметрії даними з інших джерел тощо, все це формує з розрізнених джерел інформації найповніший контекст ІБ про потоки трафіку в корпоративній мережі, доступний у 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).

За допомогою Cisco StealthWatch уся корпоративна мережа передавання даних трансформується в єдиний сенсор, що детектує атаки, аномальну поведінку тощо... Таке рішення виходить за межі корпоративної мережі, даючи змогу навіть моніторити хмарні середовища і мобільних користувачів. Рішення знає все про кожен хост і користувача в мережі, записує всі його дії в мережі (зокрема бачить мережевий трафік на рівні сигнатур застосунків), відстежує відхилення від "нормальної" поведінки (до того ж у рішенні є можливість створення профілю "правильної" поведінки (baseline) у вигляді механізму автоврядування), забезпечує зберігання цих даних, дає змогу робити вибірки з цих даних (зокрема й аналіз підозрілої активності, адже в Cisco StealthWatch уже зашифо більше ніж 100 різних алгоритмів виявлення аномалій та поведінки), попереджає адміністратора (зокрема аналіз підозрілої активності). Рішення можна використовувати як інструмент 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).

Якими ж засобами для аналітики користується це ПЗ?

— По-перше, поведінкове моделювання та поведінкові сигнатури, інакше кажучи, постійне відстеження кожного пристрою в мережі та можливість визначати базові показники нормальної та аномальної поведінки. Для кожного хоста, чи то користувач, чи то сервер, чи то роутер, будується свій baseline (ідеальна модель поведінки), відхилившись від якого, ми бачимо всі аномалії щодо цього 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 відомою Cisco Talos - величезною базою даних сигнатур відомих атак, що оновлюється по всьому світу в реальному часі.

– 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 дає змогу визначити, чи погане зашифроване з'єднання без його розшифровки (атака, небажаний трафік і C&C комунікації).

Архітектура у StealthWatch, з одного боку, трохи складніша, ніж у їхніх конкурентів, але з іншого боку, вона гранулярніша і дає змогу здійснити більш вибіркове налаштування. Як обов'язкові компоненти є Flow Collector (FC) і StealthWatch Management Console (SMC).

FlowCollector - фізичний або віртуальний пристрій, який збирає дані NetFlow і дані про застосунки за протоколом NBAR з комутаторів, маршрутизаторів і фаєрволів.

SMC - фізичний або віртуальний пристрій, який об'єднує, упорядковує і графічно представляє зібрані з FC дані. Можлива інтеграція з AD і Cisco ISE.

Як необов'язкові, але не менш цікаві пристрої виділяю FlowSensor (FS) і UDP-Director (UDP-D).

Перший може бути також як фізичним, так і віртуальним пристроєм, і є рішенням для генерації NetFlow із застарілих пристроїв або коли у вас використовуються дешеві комутатори рівня доступу. FlowSensor може забезпечити формування NetFlow-записів для всього трафіку, що надходить з використанням протоколів SPAN, RSPAN. FlowSensor здебільшого необхідний для використання технології ETA (визначення шкідливого ПЗ у шифрованому трафіку), однак починаючи з ISR і ASR серій маршрутизатори можуть працювати з ETA і без Flow Sensor.

UDP-D - фізичний пристрій, який збирає дані NetFlow і направляє їх у вигляді єдиного і стисненого потоку на FlowCollector. Як приклад, він може експортувати потік одночасно на StealthWatch, SolarWinds і щось ще. Також дозволяє знизити навантаження на Flow Collector і оптимізувати продуктивність мережі. Правду кажучи, тільки для експорту потоку на різні платформи він і потрібен. У підсумку найдорожчий компонент архітектури StealthWatch не такий вже й необхідний.

Архітектура має приблизно такий вигляд у спрощеному варіанті:

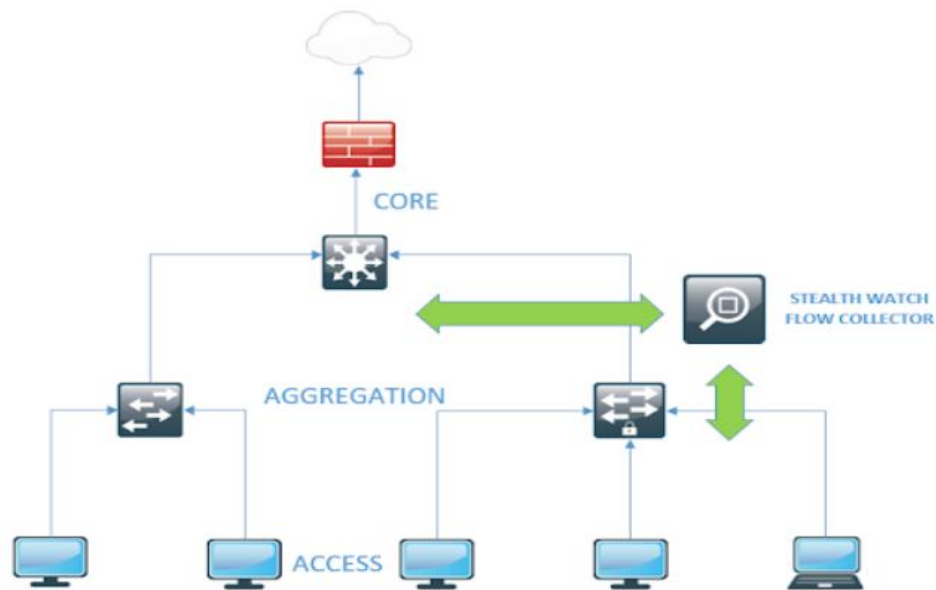


Рисунок 3.19 – Архітектура StealthWatch

Illusive Shadow. Компанія Illusive Networks була заснована 2014 року вихідцями з Unit 8200, елітного підрозділу ізраїльської кібер-розвідки. Illusive Networks бореться з найскладнішими і найнебезпечнішими націленими атаками, які змогли обійти міжмережеві екрани, IPS, пісочниці та інші засоби захисту. При цьому Illusive достовірно детектує такі атаки, не генеруючи помилкових спрацьовувань або численних алертів.

Унікальність підходу Illusive Networks полягає у створенні альтернативної реальності для зловмисника, який потрапив у корпоративну мережу. Illusive створює й активно заманює зловмисника в щільну мережу неправдивих даних, не залишаючи йому можливості дістатися до реальних ресурсів, а потім дає змогу перервати та заблокувати атаку. При цьому звичайні користувачі та IT-адміністратори не помічають змін.

Якщо ви постійно програєте вправи red team і не проходитье тести на проникнення, то зловмисники тим більше зможуть зламати вас. Illusive переміг найдосвідченіші red team, включно з Microsoft, Mandiant, Міністерством оборони США та Cisco. Тепер ця технологія доступна всім замовникам.

Illusive Networks – це модуль Attack Surface Manager активно запобігає атакам завдяки виявленню та усуненню порушень політик кешування облікових записів,

сучасна націлена атака складається з таких стадій: збір інформації, компрометація початкового хоста і закріплення там, латеральний (внутрішній) рух мережею, пошук і крадіжка даних. Illusive Networks ADS (Illusive Shadow) діє на стадії після початкового проникнення, після того, як міжмережевий екран, пісочниця й антивірус не впоралися з атакою, але до того, як зловмисник заподіяв будь-якої шкоди компанії. Deceptions Everywhere створює щільний шар неправдивих даних у корпоративній мережі, змушуючи зловмисника виявити себе під час першого ж кроку, а потім збирає хостову форензику і блокує атаку,

Illusive Networks Attacker View дає змогу поглянути на Вашу корпоративну мережу очима зловмисника, який у ній перебуває. Альтернативний погляд дає змогу отримати розуміння типової мережевої взаємодії, обрати найвірнішу стратегію захисту, виявити аномалії або порушення політик, а також спланувати оптимальне впровадження мережі приманок і пасток,

Модуль AIS дає змогу емулювати повноцінні ОС з унікальним встановленим ПЗ замовника, а також пристрої IoT, АСУ ТП і різні офісні системи,

Під час атаки на SWIFT націлені зловмисники проникають у компанію, а потім протягом 3-4 тижнів досліджують внутрішню мережу, шукають інфраструктуру SWIFT і готують атаку. Після цього здійснюється виведення грошей, причому антивіруси, міжмережеві екрани і пісочниці не бачать і не можуть протистояти таким атакам. Wire Transfer Guard, спеціалізований модуль рішення Illusive Networks, дає змогу захищати фінансові установи від почастищення атак на SWIFT-ресурси, пов'язані з шахрайським переказом грошових коштів. Illusive Networks виявляє такі атаки на ранніх стадіях, змушуючи зловмисника, який вже проник у Вашу мережу, видати свою присутність задовго до того, як він добереться до інфраструктури SWIFT, а потім блокувати його,

Модуль захисту Mainframe Guard реєструє спроби несанкціонованого доступу до мейнфреймів і захищає їх від націлених атак за допомогою неінтрузивного методу. Рішення включає можливість бачити мейнфреймні ресурси та інші критичні активи очима зловмисника, вводити зловмисників в оману завдяки новому різновиду "пасток" і "принад" для захисту мейнфреймів і їхніх

користувачів, які імітують роботу мейнфреймів і їхні екрани автентифікації. Крім того, Mainframe Guard дає змогу отримувати спеціалізовані звіти про моніторинг мейнфреймів і несанкціонованих під'єднань до них.

3.3 Системи виявлення та запобігання вторгненням, Cisco Secure IPS (NGIPS), Amazon Web Services (AWS) GuardDuty, Azure Firewall Premium IDPS, Darktrace Enterprise Immune System.

Cisco Secure IPS або система запобігання вторгненням наступного покоління (NGIPS) діє як механізм забезпечення безпеки, який забезпечує інтелектуальну інформацію та видимість мережі для захисту мережі від кібератак і загроз.

Функції Cisco Secure IPS:

- Видимість – Cisco використовує Secure Firewall Management Center для перегляду контекстних даних із мережі. Безпека мережі налаштовується та оптимізується за допомогою вхідних даних шляхом рекомендацій політик і налаштування системи Snort;
- Ефективність – нові правила політики та підписи надходять кожні дві години.
- Операційні витрати – використання автоматизації для підвищення операційної ефективності та зменшення накладних витрат, класифікує події, які викликають дії, від незначних.
- Гнучкість – доступні різні варіанти гнучкого розгортання. Він може бути розгорнутий як для внутрішньої перевірки, так і для пасивного виявлення.
- Інтеграція – впровадження не потребує серйозних змін у апаратному забезпеченні чи значного часу. Центр керування брандмауером вмикає програми безпеки та керує ними з однієї панелі. Cisco Threat Intelligence Director використовується для навігації між рішеннями безпеки Cisco.
- Високопродуктивні пристрої – серії Firepower 4100 і 9000 з портфоліо Cisco забезпечують видимість мережі, аналітику безпеки та вдосконалений захист від загроз для безпечного ІТ-середовища.
- Захист від загроз – включає виявлення вторгнень для запобігання загрозам і боротьби з атаками. Він запобігає вразливості, позначаючи й аналізуючи

підозрілі та неідентифіковані файли, а також забезпечує керування загрозами в загальнодоступних і приватних хмарах. Він також підтримує внутрішню сегментацію мережі та виправляє високопріоритетні вразливості.

Система виявлення вторгнень (IDS) пасивно відстежує та аналізує мережевий трафік на наявність будь-якої потенційної атаки вторгнення та записує дані атаки для аналізу. Система запобігання вторгненням (IPS) виконує функції IDS і автоматично обмежує атаки вторгнень.

Cisco придбала Sourcefire у 2013 році, що призвело до Cisco Firepower NGIPS. Відповідно до Gartner, Inc., IPS наступного покоління повинен мати функції IPS і деякі додаткові функції, які Firepower здатний:

1. Усвідомлення контексту в реальному часі – виявляє та надає контекстну інформацію, таку як програми, користувачі, операційні системи, уразливості, файли, загрози тощо.

2. Advanced Threat Protection and Remediation – ідентифікує, блокує, містить і усуває розширені загрози за допомогою інтегрованого AMP for Networks і Threat Grid.

3. Інтелектуальна автоматизація безпеки – автоматично пов'язує події загроз, контекстну інформацію та дані про вразливість мережі для реалізації:

- Оптимізація захисту за допомогою автоматизації оновлення політики захисту.
- Визначте постраждалих користувачів під час атаки на стороні клієнта.
- Сповіщення про порушення політики конфігурації.
- Визначте розвиток зловмисного програмного забезпечення.
- Виявлення та позначення потенційно скомпрометованих хостів за допомогою IoC.

4. Незрівнянна продуктивність і масштабованість – пристрої Cisco ASA і Firepower мають однопрохідну конструкцію з низькою затримкою, що забезпечує чудову продуктивність і масштабованість.

5. Видимість і контроль програм (AVC) – зменшуйте загрози завдяки виявленню більш ніж 4000 комерційних програм.

6. Фільтрування URL-адрес – забезпечує контроль доступу до понад 80 категорій веб-сайтів і 280 мільйонів окремих URL-адрес.

Cisco Firepower NGIPS містить такі можливості, які додатково покращують загальну безпеку:

1. Централізоване керування – централізоване керування за допомогою Cisco Firepower Management Center (FMC), єдиної панелі для керування політикою та збору подій.

2. Cisco Talos Global Threat Intelligence – інтегрується з розвідкою безпеки Cisco Talos для останніх оновлень сигнатур IPS, використовуючи найбільшу в світі мережу виявлення загроз, щоб діяти як система раннього попередження про нові загрози. Таким чином, забезпечуючи найкращу в галузі ефективність загроз.

3. Механізм виявлення Snort IPS – Snort є механізмом виявлення Firepower. Це найпотужніший у світі механізм IPS з відкритим кодом.

4. Висока доступність і кластеризація – розгортається як активна/резервна кластеризація та кластеризація всередині шасі та підтримується пристроями серії Firepower 9300.

5. Стороння екосистема та екосистема з відкритим вихідним кодом – підтримує відкритий API для інтеграції зі сторонніми продуктами.

6. Інтеграція Cisco ISE – використовується для застосування виправлення на скомпрометованому хості та безпечній кінцевій точці:

- Карантин: обмежує доступ кінцевої точки до мережі.
- Зняти карантин: видаляє статус карантину.
- Вимкнення: вимикає порт, до якого підключено скомпрометовану кінцеву точку.

Amazon Web Services (AWS) GuardDuty.

Amazon GuardDuty — це сервіс виявлення загроз, який постійно відстежує шкідливу або несанкціоновану поведінку в середовищі AWS. GuardDuty поєднує в собі машинне навчання, виявлення аномалій і виявлення шкідливих файлів, використовуючи як розробки AWS, так і сторонні джерела (GuardDuty використовує базові джерела даних для виявлення зв'язку з відомими зловмисними

доменами та IP-адресами, а також виявлення потенційно аномальної поведінки та несанкціонованої діяльності. Під час передачі від цих джерел до GuardDuty усі дані журналу зашифровані. GuardDuty витягує різні поля з цих джерел журналів для профілювання та виявлення аномалій, а потім відкидає ці журнали), що ведуть в галузі, щоб допомогти захистити акаунти, робочі навантаження та дані AWS. GuardDuty аналізує події в кількох джерелах даних AWS, включаючи журнали AWS CloudTrail, журнали потоків Віртуальної приватної хмари Amazon (Amazon VPC) та журнали запитів DNS. GuardDuty відстежує події даних Простого сервісу зберігання даних Amazon (Amazon S3), події входу до Amazon Aurora та час виконання сервісів, таких як Еластичний сервіс Amazon Kubernetes (Amazon EKS), Еластична хмара обчислень Amazon (Amazon EC2) та Еластичний сервіс контейнерів Amazon (Amazon ECS), у тому числі робочі навантаження безсерверних контейнерів в AWS Fargate.

Основні можливості:

GuardDuty точно виявляє загрози компрометації облікового запису. Швидко виявити такі загрози досить складно, якщо не ведеться безперервний моніторинг показників у режимі, близькому до реального часу. Amazon GuardDuty здатний виявляти такі ознаки компрометації облікового запису, як доступ до ресурсів AWS з незвичайного розташування у нетиповий час доби. Для програмних облікових записів AWS Amazon GuardDuty перевіряє незвичайні виклики API, наприклад спроби приховати активність облікового запису шляхом відключення функцій ведення журналів CloudTrail або спроби зробити знімки стану бази даних із шкідливої IP-адреси.

GuardDuty безперервно відстежує та аналізує дані подій облікового запису AWS та робочих навантажень клієнта, що містяться в CloudTrail, журналах VPC Flow Logs та журналах DNS. Для захисту в GuardDuty не потрібно додатково розгортати та обслуговувати програмне забезпечення чи інфраструктуру. Об'єднавши облікові записи AWS, можна виявити загрози для всіх цих облікових записів, а не для кожного окремо. Крім того, тепер не потрібно збирати, аналізувати та зіставляти великі обсяги даних AWS з кількох облікових записів. Зосередьтеся

на швидкості реагування та безпеки організації, продовжуючи розширювати та впроваджувати інновації в хмарі AWS.

GuardDuty допомагає отримати доступ до вбудованих методів виявлення вторгнення, розроблених та оптимізованих для хмари. AWS Security постійно підтримує та покращує ці алгоритми виявлення. Сервіс виявляє вторгнення наведених нижче основних категорій:

- дослідження системи . Активність, що передбачає дослідження системи зловмисником, наприклад, незвичайна активність API, підозрілі спроби входу в базу даних, сканування портів усередині VPC, незвичайні схеми невдалих запитів на вхід в систему або пошук незаблокованих портів з відомої підозрілої IP-адреси.

- несанкціонований доступ до інстансу . Активність, що вказує на несанкціонований доступ до інстансу, наприклад майнінг криптовалют, дії з управління бекдорами (C&C), час виконання Amazon EC2, шкідливе ПЗ, що використовує алгоритми генерації доменів (DGA), активність, що свідчить про відмову в обслуговуванні вихідного трафіку мережевого трафіку, незвичайні мережеві протоколи, вихідне підключення інстансу до відомих шкідливих IP-адрес, використання тимчасових даних для доступу в Amazon EC2 зовнішньою IP-адресою та ексфільтрація даних з використанням DNS.

- несанкціонований доступ до облікового запису. Перелік поширених схем, що вказують на несанкціонований доступ до облікового запису, включає виклики інтерфейсу API з незвичайного географічного розташування або з анонімного проксі-сервера, спроби відключити ведення журналів AWS CloudTrail, зміни, що пом'якшують політику паролів облікових записів, запуск незвичайних інстанцій регіоні, крадіжка облікових даних, підозріла активність при вході в базу даних та виклики інтерфейсу API з відомих шкідливих IP-адрес.

- несанкціонований доступ до кошика . Дії, що вказують на несанкціонований доступ до кошика, наприклад, підозрілі схеми доступу до даних, що вказують на неправомірне використання даних для доступу, незвичайні дії в інтерфейсі API Amazon S3 з віддаленого вузла, несанкціонований доступ до сервісу

S3 з відомих шкідливих IP-адрес та виклики інтерфейсу API для отримання даних у кошиках S3 від користувача, який не має попередньої історії доступу до кошика, чи скоєні з незвичайного розташування. Сервіс Amazon GuardDuty безперервно відстежує та аналізує події, пов'язані з даними AWS CloudTrail S3 (наприклад, GetObject, ListObjects, DeleteObject), щоб виявляти підозрілі дії у всіх ваших кошиках Amazon S3.

- шкідливе програмне забезпечення: GuardDuty може виявити наявність шкідливих програм, таких як трояни, черв'яки, криптомайнери, руткіти або боти, які можуть бути використані для погіршення робочих навантажень інстансів або контейнерів Amazon EC2 або завантажені в кошики Amazon S3 .

- несанкціонований доступ до контейнерів. Діяльність, що виявляє можливу зловмисну або підозрілу поведінку в робочих навантаженнях контейнерів, можна виявити, якщо безперервно здійснювати моніторинг та профіль кластерів Amazon EKS шляхом аналізу журналів аудиту EKS та активності під час виконання контейнера в Amazon EKS або Amazon ECS .

GuardDuty використовує три рівні серйозності (низький, середній та високий), щоб допомогти клієнтам визначити пріоритети при реагуванні на потенційні загрози. Низький рівень серйозності вказує на підозрілу чи шкідливу активність, яка була заблокована до того, як завдала шкоди ресурсу. Середній рівень серйозності свідчить про підозрілу активність. Наприклад, це може бути великий обсяг трафіку, що повертається на віддалений вузол, який ховається за мережею Tor, або активність, відмінна від схем, що раніше спостерігалися. Високий рівень серйозності вказує, що ресурс (наприклад, інстанс EC2 або набір даних для доступу користувача IAM), що розглядається, скомпрометований і активно використовується в несанкціонованих цілях.

GuardDuty дозволяє використовувати інтерфейси API HTTPS, інструменти інтерфейсу командного рядка (CLI), а також інтегрується із сервісом Amazon EventBridge для підтримки автоматичного реагування системи безпеки на виявлені загрози. Наприклад, можна автоматизувати робочий процес реагування,

використовуючи сервіс EventBridge як джерело події, що запускає функцію Lambda.

GuardDuty розрахований на автоматичне управління використанням ресурсів на основі загальних рівнів активності в облікових записах AWS, робочих навантаженнях клієнта та даних. Сервіс Amazon GuardDuty виділяє додаткові ресурси для системи виявлення вторгнення лише у разі потреби та припиняє їх використання, коли ці ресурси більше не потрібні. Сервіс має економічну архітектуру, яка гарантує наявність обчислювальної потужності, необхідної для забезпечення безпеки за мінімальних витрат. Ви платите лише за ресурси, які використовуються для виявлення вторгнення, і лише тоді, коли вони використовуються. Amazon GuardDuty забезпечує безпеку у будь-якому масштабі.

Підключити GuardDuty для одного облікового запису можна одним клацанням мишею в Консолі керування AWS або за допомогою одного виклику API. Щоб увімкнути сервіс Amazon GuardDuty для кількох облікових записів, потрібно кілька клацань мишею в консолі. У сервісі GuardDuty передбачена підтримка кількох облікових записів за допомогою інтеграції з сервісом Організації AWS. Вбудована підтримка також забезпечується у сервісі GuardDuty. Відразу після включення GuardDuty починає аналізувати безперервні потоки даних, що відображають дії облікового запису та мережну активність, в режимі, близькому до реального часу, і в потрібному масштабі. Для розгортання та керування не потрібно додаткового програмного забезпечення для безпеки, датчиків або мережевих пристроїв. Актуальна інформація про відомі загрози заздалегідь включена до сервісу та постійно оновлюється.

GuardDuty забезпечує комплексний захист контейнерних робочих навантажень у вашому обчислювальному просторі AWS, який важко реалізувати іншими методами. Незалежно від того, чи запускаєте ви робочі навантаження з контролем на рівні сервера в Amazon EC2 або робочі навантаження сучасних безсерверних додатків в Amazon ECS з AWS Fargate, GuardDuty виявляє потенційно шкідливі та підозрілі дії, надає контекст на рівні контейнера з

моніторингом часу виконання прогалини у захисті контейнерних робочих навантажень у середовищі AWS.

Azure Firewall Premium IDPS.

Система виявлення та запобігання вторгненням (IDPS) є життєво важливим компонентом сучасної стратегії кібербезпеки, розробленою для захисту мереж шляхом активного моніторингу та реагування на потенційні загрози безпеці. Серед доступних на даний момент типів IDPS, таких як на основі сигнатур і на основі аномалій, IDPS на основі сигнатур виділяється як надійний і ефективний метод виявлення відомих ризиків безпеки.

IDPS на основі сигнатур використовує базу даних сигнатур відомих аномалій, шаблонів атак і експлойтів, що робить її найкращою для виявлення відомих кіберзагроз. Цей тип IDPS має кілька переваг:

- мінімум помилкових спрацьовувань: завдяки точному зіставленню шаблонів ймовірність помилкових спрацьовувань зведена до мінімуму. Ця точність допомагає командам безпеки зосередити свої зусилля на законних загрозах.
- швидке виявлення: IDPS на основі сигнатур забезпечує швидке розпізнавання встановлених шаблонів атак, гарантуючи ідентифікацію потенційних загроз у реальному часі.
- комплексний аналіз: система проводить поглиблений аналіз різних векторів атак, виявляючи конкретні моделі зловмисної поведінки.

За своєю суттю IDPS на основі сигнатур працює шляхом порівняння мережевого трафіку з великою базою даних відомих сигнатур атак:

- перевірка пакетів : вхідні та вихідні пакети даних піддаються ретельній перевірці та аналізуються для виявлення основних характеристик.
- зіставлення сигнатур: проаналізовані пакети потім зіставляються зі сховищем розпізнаних шаблонів атак, шукаючи «сигнатуру», яка відповідає будь-якій із відомих загроз.
- генерація сповіщень: якщо система виявляє збіг, вона негайно створює сповіщення, сповіщаючи адміністраторів про потенційну загрозу.

— блокування: коли система знаходить збіг, вона негайно блокує трафік, захищаючи мережу від потенційної загрози.

Розглянемо, як Azure Firewall Premium IDPS виявляє та блокує атаки, зокрема атаки сканера. Розглянемо сценарій, коли зломисник прагне використати вразливі місця, здійснюючи атаки сканування за допомогою такого інструменту, як Nmap. Nmap, скорочення від Network Mapper, — це інструмент командного рядка Linux з відкритим кодом. Він полегшує широке дослідження мережі, дозволяючи користувачам сканувати IP-адреси та порти, виявляючи активні пристрої, доступні служби та потенційні вразливості. У нашій установці ми розгорнули наступне, щоб проілюструвати сценарій:

1. Azure Firewall Premium.
2. Веб-програма, яка працює на віртуальній машині Windows.
3. Віртуальна машина Linux для імітації атаки сканування за допомогою утиліти Nmap (також доступна версія Nmap з графічним інтерфейсом для Windows).

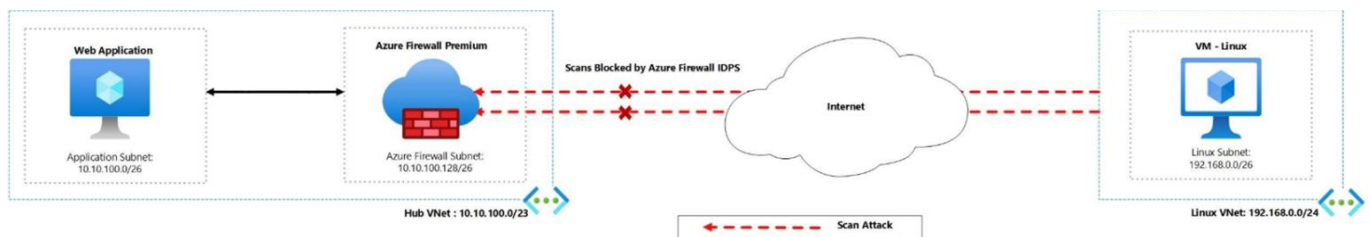


Рисунок 3.20 – Сценарій із використанням Azure Firewall Premium

Щоб отримати доступ до веб-програми, Azure Firewall Premium було розгорнуто з правилами DNAT для NAT-трафіку на загальнодоступній IP-адресі брандмауера та перекладено на серверну веб-програму.

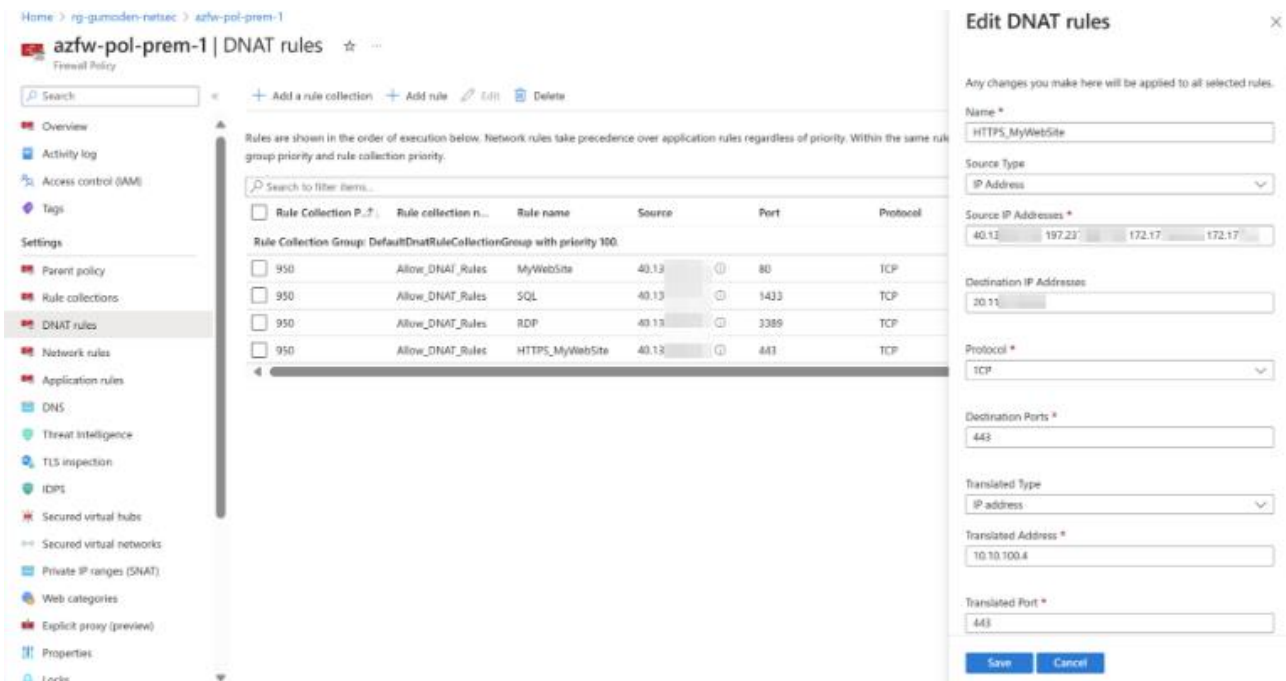


Рисунок 3.21 – Брандмауер Azure IDPS

Брандмауер Azure IDPS активується, перейшовши до Політики брандмауера, потім Параметри та натиснувши IDPS . Доступні три режими, як показано на діаграмі нижче. У наших налаштуваннях ми використовуємо IDPS у режимі оповіщення та заборони. У цьому режимі механізм IDPS сканує всі запити в рядку. Ми рекомендуємо використовувати IDPS у режимі сповіщення та заборони, щоб сканувати та блокувати будь-який підозрілий трафік.

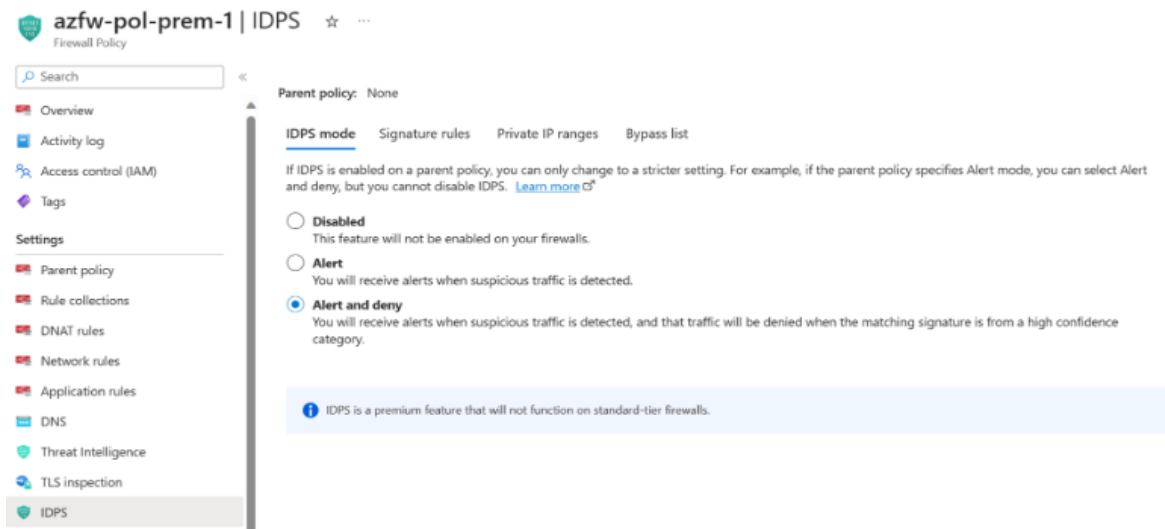


Рисунок 3.22 – IDPS

За замовчуванням є підписи, налаштовані на режим сповіщення, навіть якщо глобальна конфігурація встановлена на оповіщення та заборону . Якщо ви бажаєте

змінити режим окремих підписів, ви можете скористатися заміною підписів, вибравши та відредагувавши підписи.

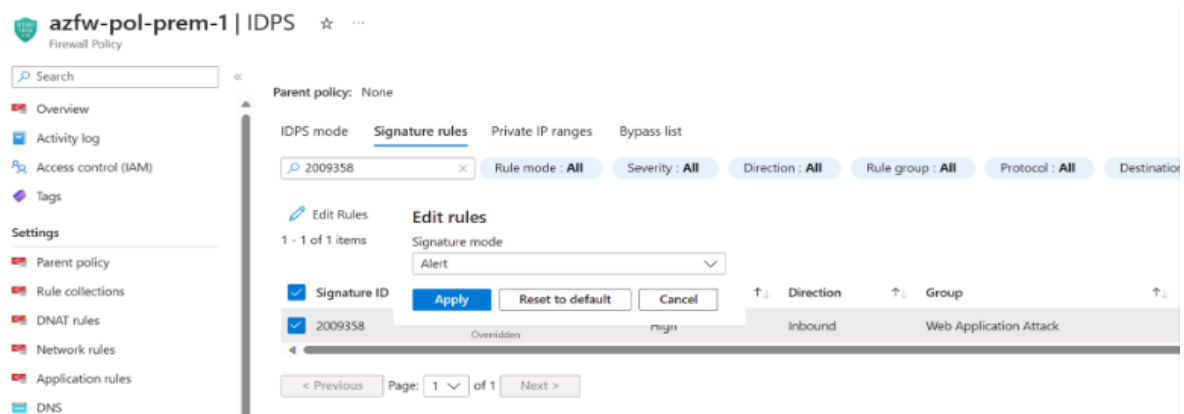


Рисунок 3.23 – Signature rules

У цій публікації блогу ми використовуємо заміну підпису для підписів нижче:

- 2009358
- 2010935
- 2023753
- 2036252

Якщо ви використовуєте кілька заміन підписів, кращий спосіб створити список підписів і побачити, які режими призначено для кожного з них, це запустити таку команду Az CLI:

```
1 | az network firewall policy intrusion-detection list --policy-name <Your Policy Name> --resource-group <Your RG Name>
```

Після успішного виконання команди результат виглядатиме так:

```
Bash
gustavo [ ~ ]$ az network firewall policy intrusion-detection list --policy-name azfw-pol-prem-1 --resource-group rg-gumoden-netsec
This command is in preview and under development. Reference and support levels: https://aka.ms/CLI_refstatus
{
  "bypassTrafficSettings": [],
  "signatureOverrides": [
    {
      "id": "2009358",
      "mode": "Deny"
    },
    {
      "id": "2010935",
      "mode": "Deny"
    },
    {
      "id": "2023753",
      "mode": "Deny"
    },
    {
      "id": "2036252",
      "mode": "Deny"
    }
  ]
}
```

Рисунок 3.24 – Результат успішного виконання команди

Налаштування веб-додатку:

Веб-програма працює на віртуальній машині Windows і прослуховує трафік на портах 80 (HTTP) і 443 (HTTPS) . На одній віртуальній машині працюють інші служби - 3389 (RDP) і 1433 (SQL Server) . Ці порти публікуються в Інтернеті, і доступ до них здійснюється через публічну IP-адресу Azure Firewall, налаштовану в правилах DNAT, проілюстрованих раніше.

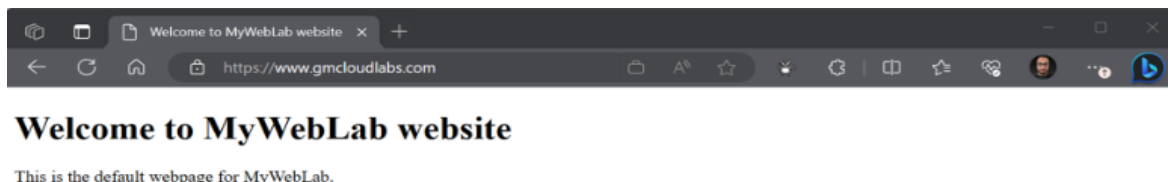


Рисунок 3.25 – Вхід у веб-додаток

Виявлення сканування:

За допомогою наведених вище налаштувань наступним кроком буде імітація атаки/виявлення сканування. На машині Linux ми запускаємо команду нижче, щоб почати сканування:

```
1 | sudo nmap <IP Address or URL> -A
```

Команда виконує повне сканування мережі за вказаною IP-адресою за допомогою інструменту Nmap. Прапорець "-A" увімкне ряд параметрів агресивного сканування, які включають:

- Виявлення операційної системи.
- Виявлення версії.
- Сканування сценаріїв (сценарій проти цілі для збору додаткової інформації та потенційного виявлення вразливостей або неправильних конфігурацій).
- Traceroute. Команда виконується, орієнтуючись на загальнодоступну IP-адресу нашої веб-програми, а результат відображається, як показано нижче:

```
AzureUser@ubuntu-vm-1:~$ sudo nmap www.gmcloudlabs.com -A
Starting Nmap 7.80 ( https://nmap.org ) at 2023-08-30 00:03 UTC
Nmap scan report for www.gmcloudlabs.com (20.110.108.130)
Host is up (0.0022s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
443/tcp    open  ssl/https
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header:
|_ Microsoft-HTTPAPI/2.0
|_ Microsoft-IIS/10.0
|_ http-title: Welcome to MyWebLab website
|_ ssl-cert: Subject: commonName=*.gmcloudlabs.com
|_ Subject Alternative Name: DNS:*.gmcloudlabs.com
|_ Not valid before: 2023-08-24T00:00:00
|_ Not valid after: 2024-09-23T23:59:59
3389/tcp   open  ms-wbt-server?
|_ ssl-cert: Subject: commonName=windows-vm-1
|_ Not valid before: 2023-08-20T19:58:30
|_ Not valid after: 2024-02-19T19:58:30
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 15 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 ... 14
15 3.00 ms 20.110.108.130

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 124.95 seconds
AzureUser@ubuntu-vm-1:~$
```

Рисунок 3.26 – Результат виконання команди

Оскільки існують правила DNAT, які дозволяють трафік від загальнодоступної IP-адреси нашої віртуальної машини Linux до різних портів, як було показано в правилах DNAT раніше, у результаті NMAP буде перелік портів і деяка інформація з віртуальної машини Windows. IDPS у цьому випадку попередить і відхилить будь-який запит, який збігається з підписами. Це буде видно в журналах брандмауера.

Якщо ми запустимо ту саму команду з вимкненим режимом IDPS або оповіщенням, ми матимемо додаткові відомості про результати, оскільки сценарії не блокуються IDPS.

```
1433/tcp open  ms-sql-s      Microsoft SQL Server 16.00.1000.00
|_ ms-sql-ntlm-info:
|_ Target_Name: windows-vm-1
|_ NetBIOS_Domain_Name: windows-vm-1
|_ NetBIOS_Computer_Name: windows-vm-1
|_ DNS_Domain_Name: windows-vm-1
|_ DNS_Computer_Name: windows-vm-1
|_ Product_Version: 10.0.20348
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ ssl-cert: Subject: commonName=windows-vm-1
|_ Not valid before: 2023-08-20T19:58:30
|_ Not valid after: 2024-02-19T19:58:30

Host script results:
ms-sql-info:
20.110.108.130:1433:
Version:
name: Microsoft SQL Server
number: 16.00.1000.00
Product: Microsoft SQL Server
TCP port: 1433
```

Рисунок 3.27 – Результат виконання команди

Тепер давайте перевіримо журнали і побачимо, які запити були відкинуті. Для перевірки журналів ми використовуємо такий KQL:

1 | AZFWIdpsSignature

2 | | where SourceIp Contains “<Public IP of the Linux VM>”

3 | | summarize by SignatureId, DestinationPort, Action, Severity, Description

4 | | order by Severity asc

Results		Chart			
SignatureId	DestinationPort	Action	Severity	Description	
> 2009358	80	drop	1	SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	
> 2009358	443	drop	1	SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	
> 2023753	443	drop	2	SCAN MS Terminal Server Traffic on Non-standard Port	
> 2010935	1433	drop	2	SCAN Suspicious inbound to MSSQL port 1433	
> 2036252	3389	drop	3	SCAN RDP Connection Attempt from Nmap	

Рисунок 3.28 – Перевірка журналів

У журналах ми можемо знайти ідентифікатори підписів, а також порт призначення, дію, серйозність і опис. Кожна сигнатура має відповідний рівень серйозності та призначений пріоритет, який вказує ймовірність того, що сигнатура є справжньою атакою.

– Низький (пріоритет 3): аномальна подія – це подія, яка зазвичай не відбувається в мережі, або реєструються інформаційні події. Ймовірність нападу низька.

– Середній (пріоритет 2): Сигнатура вказує на атаку підозрілого характеру. Адміністратор має провести подальше дослідження.

– Високий (пріоритет 1): Сигнатури атаки вказують на те, що запускається серйозна атака. Невелика ймовірність того, що пакети мають законну мету.

Система виявлення та запобігання вторгненням (IDPS) на основі сигнатур є важливим рішенням безпеки, яке допомагає ідентифікувати відомі кіберзагрози шляхом порівняння мережевих даних із заздалегідь визначеним списком відомих ознак компрометації. Це швидко, ефективно та має незначний ризик викликати помилкові тривоги.

Azure Firewall Premium IDPS відіграє вирішальну роль у припиненні значних загроз, використовуючи свою базу правил підпису, що робить його незамінним інструментом для захисту вашого середовища Azure.

Darktrace Enterprise Immune System.

Enterprise Immune System — це кібертехнологія штучного інтелекту, що самонавчається, яка виявляє нові атаки та внутрішні загрози на ранній стадії.

Створена за моделлю імунної системи людини, корпоративна імунна система вивчає та розуміє «я» для всіх і всього в бізнесі та може помітити ледве помітні сигнали передової атаки — не покладаючись на правила, підписи чи попередні припущення. Корпоративна імунна система виявляє ледве помітні ознаки нових загроз у реальному часі.

Enterprise Immune System використовує неконтрольоване машинне навчання та штучний інтелект, щоб зрозуміти все про вашу організацію. Спостерігаючи за вашими користувачами та пристроями, хмарними контейнерами та робочими процесами, він вивчає «на роботі», що є нормальним для вашої організації.

На відміну від традиційних підходів, які покладаються на чорні списки, правила та підписи, підхід імунної системи вчиться на ваших даних, формуючи індивідуальне та розвивається розуміння вашого цифрового середовища. Цей унікальний підхід дозволяє Darktrace виявляти найдосконаліші та приховані кіберзагрози, які не помічають інші інструменти. Незалежно від того, чи йдеться про новий тип програми-вимагача, чи про нову інсайдерську атаку, корпоративна імунна система виявляє загрозу на самих ранніх стадіях.

Кіберзагрози можуть виникати будь-де – у вашій хмарі чи SaaS, електронною поштою чи на пристроях Інтернету речей у вашій мережі. Enterprise Immune System проливає світло на всі ці середовища, включаючи Salesforce, Office 365 і SharePoint, AWS і Microsoft Azure. Це означає, що організації отримують переваги від уніфікованого уявлення про всю свою цифрову власність, а не лише про її частину, і можуть швидко протистояти загрозам, що виникають.

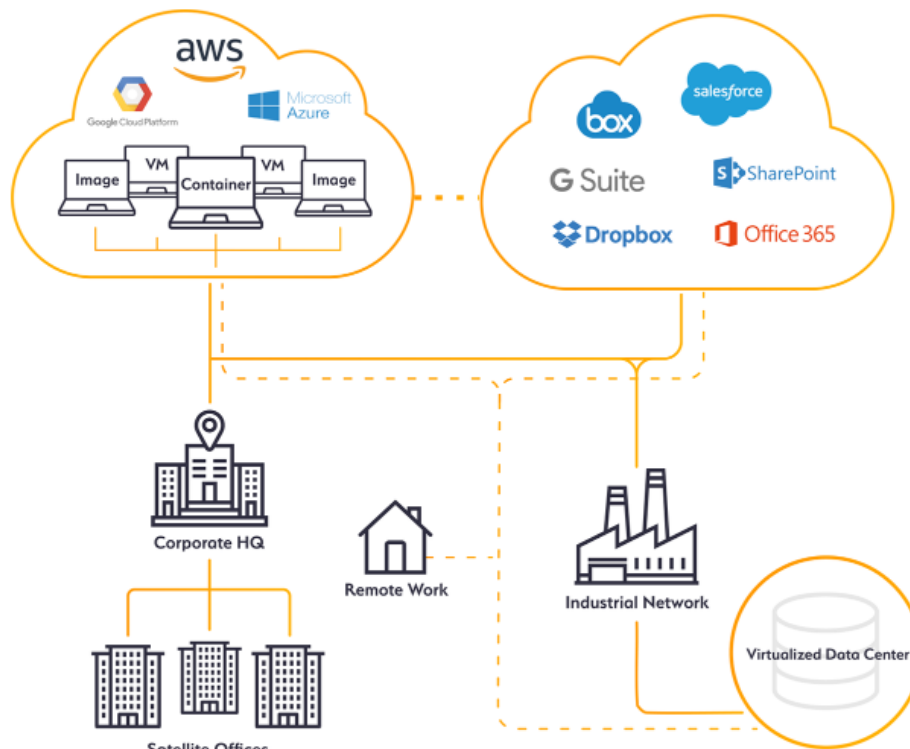


Рисунок 3.29 – Enterprise Immune System

Enterprise Immune System використовує відкриту та розширювану архітектуру, щоб плавно підключатися до вашої різноманітної екосистеми в міру її розвитку. З інтеграцією в один клік і користувацькі шаблони, платформа може миттєво вводити нові форми телеметрії та ділитися спеціальними знаннями штучного інтелекту в установлених робочих процесах.



Рисунок 3.30 – Enterprise Immune System

Вивчаючи нормальні закономірності та відкриваючи нові загрози, Enterprise Immune System представляє основну здатність ширшої платформи самонавчання.

Продукт не тільки взаємодіє з Cyber AI Analyst, щоб забезпечити автономні розслідування, але й забезпечує адаптивну структуру автономного реагування через Darktrace Antigena. Завдяки Antigena платформа може реагувати на самонавчаючі виявлення та нейтралізувати нові атаки з динамічною та хірургічною точністю. Усі три можливості заземлені у фундаментальній технології Cyber AI і може бути плавно розширена для захисту промислових середовищ, кіберфізичних систем і платформ електронної пошти.

Робота вдома підвищила профіль ризику для компаній, оскільки співробітники могли порушити політику або ненавмисно наражати корпоративні системи на нові кіберзагрози, а кількість атак різко зросла. Оскільки офіси починають знову відкриватися, служби безпеки стурбовані тим, що працівники, які підключалися до корпоративних систем із домашньої мережі, повернули потенційно зламані пристрої на робоче місце. Корпоративна імунна система Darktrace захищає динамічну робочу силу, вивчаючи їх моделі роботи, навіть якщо вони змінюються день у день. Незалежно від того, чи перебувають співробітники в офісі чи працюють віддалено, використовують Teams або Zoom, підключаються до хмари чи покладаються на електронну пошту, кіберштучний інтелект Darktrace швидко вивчає «нову нормальність», адаптуючись до середовища, що швидко змінюється, і автоматизує та розширює команди безпеки.

ВИСНОВКИ

У правовій традиції захист персональних даних трактується як одна з безумовних підстав забезпечення фундаментального права людини на недоторканність її особистого життя, яке, своєю чергою, є засадничим для сучасної демократії з її приматом поваги до прав і гідності людини. Нині цей погляд є загальновизнаним у світі: недоторканність приватного життя, у т.ч. особистої інформації людини, як одне з її основних прав закріплена в найважливіших міжнародних актах сучасності.

Тотальна комп'ютеризація телекомунікацій, систем транспортування, фінансів, обліку населення, медичного обслуговування, численних баз даних постійно збільшує кількість та якість інформації, що опрацьовується стосовно кожної особи, причому зазвичай без її відома. Існує та постійно вдосконалюється низка технологій для датамайнінгу та створення індивідуальних «онлайн-портретів» на основі збору та аналізу всіх відомостей, що мають будь-який (хай і непрямий) стосунок до користувачів. Рівень «деанонімізації» користувачів у сучасному онлайн-середовищі стає майже стовідсотковим, навіть якщо вони дотримуються вимог безпеки.

Додаткові й дуже серйозні ступені ризику щодо безпеки даних несуть у собі елементи новітньої третьої ІТ-платформи, яка нині активно впроваджується у світі і принципово орієнтована на: а) зберігання основної частини інформації користувачів не на особистих фізичних носіях, а у віртуальному середовищі («хмарові» сервіси); б) повсюдний швидкісний безпроводний доступ до інтернету. Практика свідчить, що на цей час така модель зберігання та оброблення інформації не може гарантувати особі (а) постійний і стабільний доступ до її персональних даних, (б) недоторканність цих даних, (в) контроль за їх обробленням (г) точні відомості про їх місцезнаходження. Іншими словами, проб лематично гарантувати фундаментальне право особи на «прайвесі» (приватність).

Загалом сьогодні суть проблеми захисту персональних даних у кіберпросторі визначається процесами, що є тісно пов'язаними та взаємодоповнюваними: •

перманентне і швидке збільшення кількості персональних даних громадян у публічному та/чи несанкціонованому ними доступі; • перманентне зменшення для пересічного громадянина реальних можливостей контролю збору й оброблення його власних ПД. Поки що ці дві тенденції є прогресуючими і стабільними рівно настільки, наскільки сталим є розвиток самого кіберпростору, незважаючи на численні скандали, судові позови, суспільні та законодавчі ініціативи, вимоги дотримання права і вдосконалення систем безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України "Про інформацію". <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
2. Закон України "Про захист персональних даних". <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
3. Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., Толюпа, С. В. (2015). Інформаційна та кібербезпека: соціотехнічний аспект : підручник. ДУТ
4. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с
5. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с.
6. Грайворонський М.В., Новіков О.М. Безпека інформаційнокомунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608с.
7. А. В. Жилін, О. М. Шаповал, О. А. Успенський ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ Навчальний посібник Київ — 2020
8. ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СУЧАСНОМУ КІБЕРПРОСТОРІ: ПРАВОВІ ТА ТЕХНІКО-ТЕХНОЛОГІЧНІ АСПЕКТИ НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ Серія «Інформаційні стратегії». Випуск 3
9. Грайворонський М. В., Новіков О. М. Г14 Безпека інформаційно-комунікаційних систем. — К.: Видавнича група ВНУ
10. Барнич, М. Б. Забезпечення захисту персональних даних при обробці та передаванні в ІТ-інфраструктурі організації / Барнич Мар'ян Богданович // Інженерія програмного забезпечення і передові інформаційні технології (SoftTech-2023)
11. Кібербезпека: стратегії атак та оборони Ердаль Озкая, Юрій Діогенез Вид. Birmingham-Mumbai, 2020 p.
12. Як стати хакером Едріан Прутяну Вид. Birmingham-Mumbai, 2020p.

13. Ковтух Є. В. Кібербезпека у публічному секторі. Харків: Колегіум, 2021. 271 с.
14. Центр безпеки та конфіденційності Microsoft
<https://www.microsoft.com/uk-ua/trust-center>.
15. Абдалла А., Альошин Г., Вдовиченко І. та ін. Кібербезпека та інформаційні технології. Харків: Діса плюс, 2020. 379 с
16. “Тестування комп’ютерних систем на проникнення» для студентів спеціальності 125 «Кібербезпека» – Тернопіль: ТНЕУ, 2019. 119 с.