Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління _____
(повна назва)

Кафедра _____Безпеки інформаційних технологій _____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____перший (магістерський)_____

__Методи виявлення та усунення вразливості в інформаційній системі за допомогою SIEM
(тема)

Виконав:

студент _2_ курсу, групи _БІКСзм–20–2____

____Риков О.А._____
(прізвище, ініціали)

Спеціальність _____125 Кібербезпека _____
(код і повна назва спеціальності)

Освітня програма ___«Безпека інформаційних і комунікаційних систем»____
(повна назва освітньої програми)

Керівник _доцент Сєвєрінов О.В._
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____Халімов Г.З.__
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет_____Комп'ютерної інженерії та управління _____

Кафедра_____Безпеки інформаційних технологій_____

Рівень вищої освіти_____перший (магістерський)_____

Спеціальність_____125 Кібербезпека _____
(код і повна назва)

Освітня програма_____«Безпека інформаційних і комунікаційних систем»___
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____»_____ 20 ___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЙНУ РОБОТУ

студентові_____Рикову Олександру Андрійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи Методи виявлення та усунення вразливості в інформаційній системі за допомогою SIEM_____
затверджена наказом по університету від 25 жовтня 2021 р. № 166Стз
2. Термін подання студентом роботи до екзаменаційної комісії _16_12_____2021 р.
3. Вихідні дані до роботи __алгоритми автентифікації: S / Key,Token Password Authentication, PPP, TACACS +, RADIUS; технології цілісності і конфіденційності : SSL, SSH, SOCKS, IPSec, X.509; методи віддаленого доступу до VPN: L2F, Point–to–Point Tunneling Protocol, L2TP.; аналіз вразливостей._____
_____
_____
_____
_____
_____
_____
_____
_____
_____

4. Перелік питань, що потрібно опрацювати в роботі _____
Мережеві атаки.
Протоколи захисту.
Виявлення нових вразливостей у SonarQube та Grafana за допомогою SIEM .
_____
_____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _презентаційний матеріал у вигляді слайдів _____
_____
_____
_____
_____
_____
_____
_____
_____
_____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування Розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	1.09.2021	Виконано
2	Робота з джерелами за тематикою роботи	1.09.2021– 1.10.2021	Виконано
3	Вивчення основних понять в сфері загроз безпеки	1.10.2021-22.10.2021	Виконано
4	Аналіз загроз безпеки від мережевих атак	22.10.2021-29.10.2021	Виконано
5	Аналіз безпеки від мережевих атак	29.10.2021-6.11.2021	Виконано
6	Аналіз SIEM - систем	6.11.2021-12.11.2021	Виконано
7	Виявлення нових загроз	12.11.2021-25.11.2021	Виконано
8	Оформлення пояснювальної записки	25.11.2021-15.12.2021	Виконано

Дата видачі завдання _1____ ____вересня_____2021 р.

Студент _____
(підпис)

Керівник роботи _____ доцент Сєвєрінов О.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до магістерськоі кваліфікаційної роботи: 73 с., 17 рис., 15 джерел.

ІНФОРМАЦІЙНА БЕЗПЕКА, МЕРЕЖЕВА АТАКА, ЗАГРОЗА, КЕРУВАННЯ ДОСТУПОМ , SIEM , IPS/IDS, ПРОТОКОЛИ ЗАХИСТУ

Об’єкт дослідження – мережеві вразливості інформаційної системи.

Предмет дослідження – процес захисту від мережевих вразливостей.

Мета роботи – розробити метод виявлення та захисту від мережевих вразливостей в інформаційний системи

Методи дослідження – аналіз літературних джерел та практика на виробництві.

Результати роботи викладені у вигляді описання моделей мережевих атак та методів виявлення. Детально розглянути сучасні протоколи захисту інформації та отримані дані, можливо бути використати для навчання спеціалістів з інформаційної безпеки та інших осіб, які професійно зв’язані з захистом інформації в галузі інформаційної безпеки. Результати роботи можуть бути використані для створення захисту інформації в підприємствах з можливістю подальшого використанні та удосконаленню.

ABSTRACT

The Explanatory note to the master's qualification work: 73 fs., 17 fig., 15 sources.

INFORMATION SECURITY, NETWORK ATTACK, THREAT, ACCESS CONTROL, SIEM, IPS / IDS, PROTECTION PROTOCOLS

The object of research is network vulnerabilities of the information system.

The subject of research is the process of protection against network vulnerabilities.

The purpose of the work is to analyze the security of the information system with the help of SIEM-systems from network attacks

Research methods - analysis of literature sources and practice in the workplace.

The results are presented in the form of a description of network attack models and detection methods. It is possible to use in detail the modern protocols of information protection and the received data, it is possible to use for training of experts in information security and other persons who are professionally connected with protection of information in the field of information security. The results of the work can be used to create information security in enterprises with the possibility of further use and improvement.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІБ– інформаційна безпека

RFC– Request for Comments

ПЗ – програмне забезпечення

OTP – One–Time Passwords

SSH– Secure Shell

SSL– Secure Socket Layer

ВПЗ – вірусне програмне забезпечення

DoS – Denial of Service

TCP– Transmission Control Protocol

RFC – Request for Comments

DoS – Denial of Service

ICMP – Internet Control Message Protocol

DNS – Domain Name System

IDS – intrusion detection system

IPS – intrusion prevention system

DMZ – Demilitarized Zone

PPP – Point–to–Point Protocol

LCP – Link Control Protocol

NCP– Network Control Protocols

PAP– Password Authentication Protocol

CHAP – Challenge Handshake Authentication Protocol

EAP – Extensible Authentication Protocol

NAS – Network Access Server

AAA – Authentication, Authorization, Accounting

WAIS – Wide Area Information Server

ESP – Encrypting Security Payload

VPN – Virtual Private Network

IKE – Internet Key Exchange

CA – Certificate Authority

PPTP – Point–to–Point Tunneling Protocol

GRE – Generic Routing Encapsulation

PoE – Power over Ethernet

SDM – Security Device Manager

NAC – Network Admission Control

ЛОМ – локальна обчислювальна мережа

CME – CallManager Express

SRST – Survivable Remote Site Telephony

ACS – access control server

DHP – Dynamic Host Configuration Protocol

SDEE– Security Device Event Exchange

SDF– Signature Detection File

CBAC– Context–Based Access Control

ISP– Internet Service Provider

ВСТУП

Будь-яка інформаційна система містить таку інформацію, розголошення якої третім особам може завдати шкоди її власнику або особі, до якої ця інформація відноситься. Питання інформаційної безпеки в компаніях та організаціях, в яких обробляється інформація з обмеженим доступом, стає актуальним.

Нові інформаційні технології успішно впроваджуються в усіх сферах діяльність людини. Поява глобальних і локальних мереж передача даних надала нові можливості для швидкого обміну інформації. Через всесвітню павутину зі стеком Протоколи TCP/IP і єдиний адресний простір не поєднуються тільки корпоративні та відомчі мережі, а й звичайні користувачі, які мають прямий доступ до Інтернету зі свого персонального комп’ютера. У той же час природне бажання користувачів мати постійний доступ до своєї особистої, домашню та ділову інформацію діяльності та бути впевненим у неможливості його протиправної діяльності використання. Проблема забезпечення безпеки суб’єктів інформаційні відносини, захист своїх законних інтересів при використання інформаційних систем, які зберігаються та обробляються їхня інформація вимагає постійної уваги та пошуку шляхи її вирішення.

Сьогодні для позначення часто використовують термін «інформація». особливий продукт, вартість якого часто перевищує собівартість комп'ютерну систему, в якій вона існує. Коли появі загрози, пов'язані з можливістю втрати, спотворення, розкриття конфіденційність і витік певної інформації, організації або держава в цілому може втратити не тільки великі суми грошей, але репутація на політичному та економічному рівні.

З розвитком і ускладненням засобів, методів і форм автоматизація процесів обробки інформації зростає і на рівні загрози використаним інформаційним технологіям. Ось чому шляхом використання сучасних методів і засобів захисту

цілісність і конфіденційність інформації (антивірусні програми, брандмауери, програмні та апаратні продукти для захисту всієї інформацію від несанкціонованих атак та вірусних атак тощо), ви можете забезпечити безпеку за допомогою автоматизованої система та автоматизований персонал робоче місце користувача.

У мережі не повинно бути інформації, розкриття якої могло б мати серйозні наслідки. Слід завжди враховувати, що в будь-який момент ця інформація може бути перехоплена, змінена або стати недоступною. Рішення полягає у чіткому розмежуванні інформації, що має життєво важливий інтерес для суб'єктів - користувачів - та створенні спеціалізованих систем для її обробки.

Успіх застосування систем захисту інформації залежить від наявності у них засобу керування режимами роботи та виконання функцій, значно спрощує встановлення, налаштування та експлуатація захисних засобів. У запропонованій дипломній роботі розглянуто можливі види атак персональний комп'ютер і локальна мережа, обидва в мережах та з Інтернету.

Метою данної работи є запропоновати методи та засоби інформаційної безпеки, методичні рекомендації для встановлення та експлуатація апаратних і програмних засобів захисту ПК.

1 МЕРЕЖЕВІ АТАКИ

Мережеві атаки різноманітні, як і системи, на які вони спрямовані. Деякі атаки дуже складні, а інші, можливо використати через звичку користувача системи, навіть не передбачають наслідків. Щоб оцінити типи атак, потрібно зрозуміти деякі обмеження, які насправді застосовуються до TCP/IP. Інтернет був розроблений для спілкування між державними установами та університетами для полегшення процесу навчання та дослідження. Як наслідок, у специфікаціях версій Інтернет-протоколу не було вимог безпеки. Через це багато реалізацій IP спочатку є вразливими. Багато років потому, після багатьох записів (запитів RFC), нарешті були представлені засоби захисту IP. Однак з моменту розробки захисту IP до загальної реалізації було додано ряд методів, послуг і мережевих продуктів, які зменшують ризики, властиві протоколу. Далі ми коротко обговоримо типи атак, які зазвичай використовуються проти мереж і способи протидії їм . Тобто сканування пакетів, шахрайство, відмова в обслуговуванні, середні людські атаки, мережевий аналіз, переадресація портів, трояни, атаки на рівні програмного забезпечення, атаки на паролі та соціальна інженерія.

1.1 Кіберзагрози: підсумки 2 кварталу 2021 року

У порівнянні з першим кварталом 2021 року кількість атак зросла лише на 0,3%. Темпи зростання цього показника сповільнилися; цього слід було очікувати, оскільки компаніям вдалося адаптуватися до роботи в умовах пандемії коронавірусу, включаючи заходи щодо захисту периметра мережі та систем віддаленого доступу.

Обсяг цілеспрямованих атак зростає з кварталу до кварталу. У другому кварталі 77% атак були цільовими. Відсоток інцидентів, під час яких

кіберзлочинці націлювали на осіб, залишився на тому ж рівні, що й у попередньому кварталі – 12%.

Атаки зловмисника за допомогою програмного забезпечення залишаються на вершині арсеналу кіберзлочинців. Порівняно з I кварталом 2021 року частка цього методу зросла на 15 процентних пунктів і становить 73%. Ми бачимо, що тенденція до розробки шкідливого програмного забезпечення, спрямованого на системи Unix, інструменти віртуалізації та оркестраторів, нарешті прижилася.

У другому кварталі були побиті всі рекорди за кількістю атак з використанням шкідливих програм: на них припадало 69% усіх атак з використанням шкідливих програм. Пік зростання припав на квітень. Однак на початку травня зловмисники атакували найбільшу трубопровідну систему США Colonial Pipeline та поліцейське управління округу Колумбія, привернувши увагу правоохоронних органів. В результаті кіберзлочинці почали змінювати підхід до атак і вносити зміни в партнерські програми. Ми припускаємо, що в довгостроковій перспективі оператори програм-вимагачів повністю відмовляться від партнерів як окрему роль і самі контролюватимуть команди продажів.

Власники пристроїв QNAP мали бути насторожі у другому кварталі. Ці пристрої дають змогу об’єднувати великі обсяги даних від компаній та окремих осіб, і тому є дуже цінними для зловмисників. У більшості випадків клієнти QNAP зазнавали атаки за допомогою програм-вимагачів, таких як AgeLocker і eCh0raix.

Частка атак на державні установи в усіх атаках на організації різко зросла з 12% у першому кварталі 2021 року до 20% у другому кварталі. 73% інцидентів зі зловмисним програмним забезпеченням пов’язані з розповсюдженням кіберзлочинців програм-вимагачів. Новий завантажувач Tomiris був виявлений PT ESC; Шкідливе програмне забезпечення має функції закріплення і може надсилати зашифровану інформацію через робочу станцію на сервер, який контролюють зловмисники.

Ландшафт кіберзагроз для індустрії роздрібної торгівлі змінився. У другому кварталі ми помітили зменшення атак Magecart і збільшення частки атак, під час яких кіберзлочинці використовували програми-вимагачі. Якщо раніше кіберзлочинці намагалися вкрасти дані, то тепер вони шукають пряму фінансову вигоду від атак.

Промисловий сектор також особливо сильно постраждав від розповсюджувачів програм-вимагачів у цьому кварталі. Вони були причетні до 80% інцидентів зі зловмисним програмним забезпеченням. Поширеним стало використання хакерства: частка цього методу зросла з 29% до 34%. PT ESC виявив нове зловмисне програмне забезпечення для дистанційного керування B-JDUN, яке було виявлено під час атаки на енергетичну компанію [1].

Для захисту від кібератак спочатку рекомендуємо вам дотримуватися загальних рекомендацій щодо забезпечення особистої та операційної кібербезпеки. Враховуючи особливості атак у цьому кварталі, наполегливо рекомендуємо своєчасно встановлювати оновлення безпеки. Крім того, радимо ретельно розслідувати всі основні інциденти, щоб виявити точки небезпеки та слабкі місця, якими скористалися зловмисники, а також вчасно переконатися, що зловмисники не залишили для себе жодних закутків. Завдяки сучасним інструментам безпеки, наприклад брандмауерам веб-додатків для захисту веб-ресурсів, ви можете підвищити безпеку на периметрі компанії. Щоб запобігти зараженню шкідливим програмним забезпеченням, ми рекомендуємо використовувати пісочниці, які аналізують поведінку файлів у віртуальному середовищі та виявляють шкідливу активність.

Кількість атак зросла на 0,3% порівняно з першим кварталом 2021 року. Частка атак, спрямованих на компрометацію комп’ютерів, серверів і мережевих пристроїв, зросла з 71% до 87%, що обумовлено збільшенням атак програм-вимагачів. Також зросла частка атак на прибуток (з 43% до 59%). Кіберзлочинці найчастіше нападають на медичний, державний та промисловий сектори.

Під час нападу кіберзлочинців, швидше за все, керуються мотивами збору даних. Частка порівняно з I кварталом 2021 року зросла (рис. 1.1).

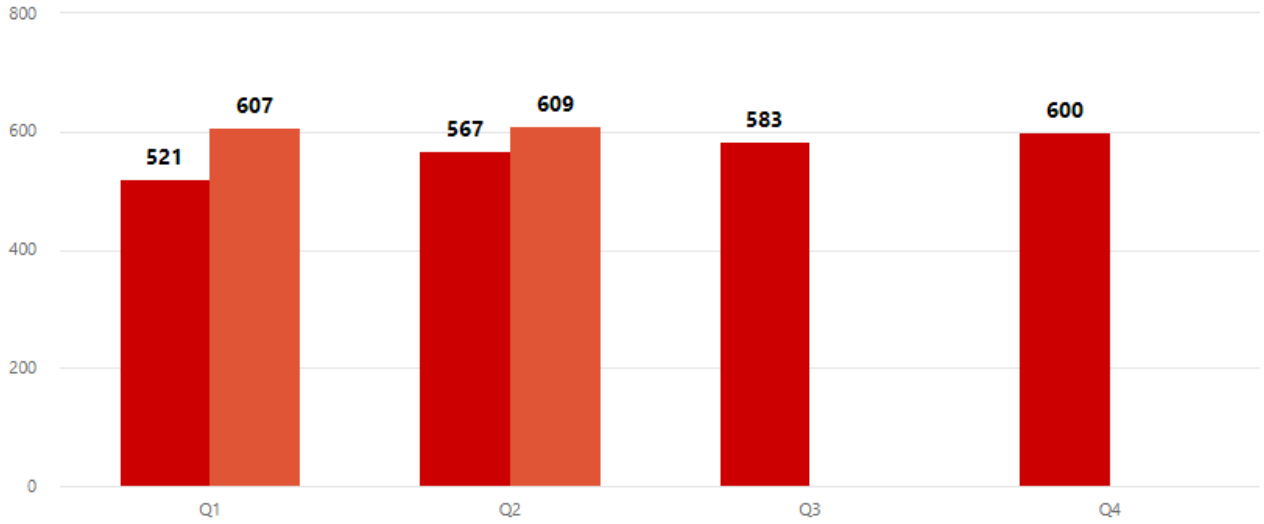

Рисунок 1.1 – Кількість кіберзагроз в 2020 та 2021 році

1.2 Типи вкрадених даних

Інститут SANS і Національний центр захисту інфраструктури (NIPC) ФБР опублікували спільну заяву, в якій стверджують: «Інтернет не готовий до атак, і найближчим часом кібератаки кібер-терористів будуть посилюватися. «Поки що всі ці прогнози повністю підтвердилися. Кількість хакерських атак зростає неймовірно швидко, виявляються нові діри в системі та програмному забезпеченні безпеки, а спалахи вірусів вже загрожують Інтернету в цілому.

За таких обставин кожен користувач ПК, який має якесь відношення до комп'ютерних мереж, має шанс стати жертвою комп'ютерного злочину. Але що саме спонукає хакерів до незаконної діяльності? Щоб зрозуміти це та багато іншого, варто спочатку зрозуміти мотиви дій кіберзлочинців; зрозуміти, на що саме можна націлити вас.

Звичайно, майже кожен очікує, що не стане жертвою грабіжника. Але хакери дозволяють власним міркуванням керувати ними, і в більшості випадків їм зовсім байдуже думки та бажання звичайних користувачів. Отже, які основні

мотиви хакерських атак на корпоративні комп’ютерні мережі, окремі сервери і навіть приватні комп’ютери. Сьогодні фахівці з комп’ютерної безпеки виділяють такі групи мотивів.

Цікавість є однією з основних мотивацій хакерської діяльності. Кожен талановитий хакер допитливий за визначенням, ну, якщо сюди включити молодь. Крім того, в більшості випадків цікавість абсолютно безкорислива, так що «просто допитливий» хакер зазвичай не завдає великої шкоди своєму об’єкту в напад. Вважається, що існує три види хакерської цікавості. Перший тип пов'язаний з процесом проникнення в комп'ютерну мережу або окремий сервер, тобто подолання систем безпеки. У той же час фактичний вміст мішені мало цікавить хакера; йому важливіше перевірити «міцність» захисту, перевірити свій інтелект. За великим рахунком, така атака не представляє особливих небезпек, особливо якщо хакер дотримується принципів хакерської етики та повідомляє системного адміністратора про виявлені вразливості.

Другий тип цікавості пов’язаний саме з вмістом атакуваної системи або можливостями, які вона пропонує. Наприклад, у корпоративній мережі хакера можуть цікавити бази даних клієнтів, фінансова звітність, вихідні коди програмного забезпечення, яке розробляється, тощо. Це вже дуже небезпечний курйоз, оскільки отримана таким чином інформація згодом може бути використана для вимагання, фінансового шахрайства чи іншої протиправної діяльності. Крім того, самому хакеру взагалі немає необхідності використовувати інформацію таким чином. Відомо багато випадків, коли конфіденційна інформація, отримана комп’ютерними хакерами, потрапляла до рук представників кримінального світу з усіма наслідками.

Третій тип курйозу по праву можна назвати ідеєю Інтернету. І хакери в класичному розумінні не мають до цього нічого спільного. Справа в тому, що багато користувачів, які цікавляться глибинами всесвітньої павутини, не рідко знаходять сайти з різноманітними програмами - цікаві, але не завжди нешкідливі. Результати їх впровадження та використання часто непередбачувані. Ви можете

знайти все, від троянських коней і сніферів до інструментів DDoS-атак. Тож якщо ви любите досліджувати невідомі програми, ви ризикуєте не лише собою, а й своїми колегами, друзями, партнерами по електронній пошті та навіть абсолютно невідомими нормальними користувачами Інтернету [1].

Матеріальну вигоду можна назвати якщо не найпоширенішим, то принаймні найзрозумілим мотивом хакерських атак.

Справа в тому, що комерційні інтернет-ресурси, як правило, мають не тільки бажання бути добре захищеними від злому, а й фінансові можливості зробити це на найвищому рівні. Це, в свою чергу, вимагає надзвичайно високого рівня професіоналізму від потенційних крекерів.

Хакерські атаки, спрямовані на матеріальну вигоду, також можна розділити на кілька типів. Перший тип — це атаки, які при успішній реалізації приносять хакеру «прямо» гроші. З цією метою зламуються бази даних з метою крадіжки даних кредитної картки, замовляються товари на основі неправильних даних в інтернет-магазинах, шахрайства на веб-аукціонах, «коригуються» банківські перекази, зламуються системи електронних платежів тощо.

Другий тип атаки – це викрадення інформації, яка потім продається. Як правило, такі дії проводяться «на замовлення», і хакер заздалегідь знає, де знаходиться потрібна інформація і скільки він за неї отримає. Третій тип – це атаки, які мають на меті завдати шкоди конкуренту і таким чином отримати перевагу на ринку. Такі акції можуть бути самими різними. Наприклад, ви можете «залити» веб-сервер конкурента, щоб уповільнити його електронний бізнес або дискредитувати його в пресі. Вони можуть вкрасти або просто знищити важливі дані. Є можливість проникнути на поштовий сервер конкурента і розсилати підроблені листи від його імені. Ви можете опублікувати компрометуючий прес-реліз на їхньому веб-сайті. Взагалі тут все обмежується виключно уявою замовника про таку дію.

Дуже важливі мотиваційні фактори, силу яких не варто недооцінювати. Деякі психологи навіть ставлять їх на перше місце – перед матеріальними

благами. Не секрет, що багато комп'ютерних спеціалістів замкнуті в собі, мають певні труднощі в спілкуванні, мають відносно низьку самооцінку. Злом комп'ютерних систем для таких людей – це спосіб піднятися як у власних очах, так і в очах оточуючих, а головне – «колег по професії». Саме бажання стати відомим керує тими, хто проводить «дефайсинг» веб-сайтів (заміна домашньої сторінки) та інші резонансні просування.

Усі три мотиви є безпосередніми причинами явища під назвою кібертероризм. Причини цього можуть бути самими різними, але методи реалізації не відрізняються особливою різноманітністю. До них належать написання вірусів, злом новин, атаки (у тому числі з використанням технології DDoS) на веб-сайти великих корпорацій та державних установ різних країн, поширення «альтернативної» інформації про поточні події, спроби доступу до Інтернету в цілому паралізують або будь-яку доменну зону.

Давайте розглянемо мотиви один за одним. Політика була і є одним із головних мотивів хакерських атак. Майже всі політичні події останнього десятиліття супроводжувалися «боротьбою» у кіберпросторі. Це югославські конфлікти та війни в Чечні, Афганістані, Іраку та політичне протистояння між США та Іраном, Північною Кореєю та Китаєм. Відомо, що політичні групи (особливо радикальної орієнтації) активно набирають комп'ютерних експертів – перш за все для протидії конкурентам та активнішого поширення «правильної» інформації в Інтернеті. Ну, а крайні екстремісти та міжнародні терористи намагаються безпосередньо використовувати хакерів для здійснення терористичних актів. Конкретних випадків такого тероризму, які були доведені в суді, небагато, але надходить багато різних «сигналів».

Ідеологія як один із мотивів дії хакерів також далека від політики. Відомо, що багато IT-спеціалістів прихильні до ліберальної ідеології. Отже, «ідеологічні» атаки з боку хакерів – це, як правило, або атаки антиглобалістів на транснаціональні корпорації та уряди найбагатших країн, або дії хакерів, які виступають проти посягань на свободу всюди (показовим прикладом є Китай).

Інша специфічна реалізація ідеології свободи – боротьба з приховуванням будь-якої інформації ким завгодно. «Інформація має бути безкоштовною!» – кажуть хакери по всьому світу, і під таким гаслом вони проникають в різні бази даних і поширюють отримані таким чином дані у відкритому доступі в Інтернеті. Вони також створюють однорангові мережі і всіляко допомагають порушувати авторські права [2].

Тепер щодо релігійних мотивів. Відомо, що тоталітарні секти в різних країнах світу залучають до своєї діяльності висококваліфікованих IT-спеціалістів. Це відбувається з кількох причин. По-перше, поповнити свій касовий апарат через комп'ютерне шахрайство. По-друге, заохочувати до більш активного поширення своїх ідей в Інтернеті. І по-третє, і найгірше, за здійснення терактів. Але секти – це не вся релігія. Бувають випадки, коли хакер починає діяти занадто глибоко «пронизаний» ідеями цілком традиційної конфесії. Однак це більше цікавить психіатра.

Ці мотиви зазвичай пов'язані з хакерською атакою на мережу компанії зсередини. Простіше кажучи, це класичний саботаж. Причини можуть бути різними: відсутність підйому по службових сходах, низькі зарплати, занадто низький статус в ієрархії компанії, догана з боку керівництва - все це може стати тригером. Навряд чи варто пам'ятати, що потенційна деструктивність внутрішньої атаки набагато перевершує «зовнішню». Крім того, в ролі «внутрішнього хакера» може виступати системний адміністратор або навіть співробітник відділу інформаційної безпеки. На жаль, таких випадків багато (рис. 1.2). Як зазначають спеціалісти кадрових агентств, IT-спеціалісти у «звичайній» компанії (тобто коли інформаційні технології не є основним профілем роботи) зазвичай відчувають недооцінку і, насамперед, не бачать для себе перспектив. Такий фахівець часто дотримується думки, що рівень його заробітної плати і виявлена до нього повага зовсім не відповідають обсягу його знань і навичок. Щоб усунути таку загрозу комп'ютерного саботажу, рекомендується звернутися за допомогою до персональних психологів.

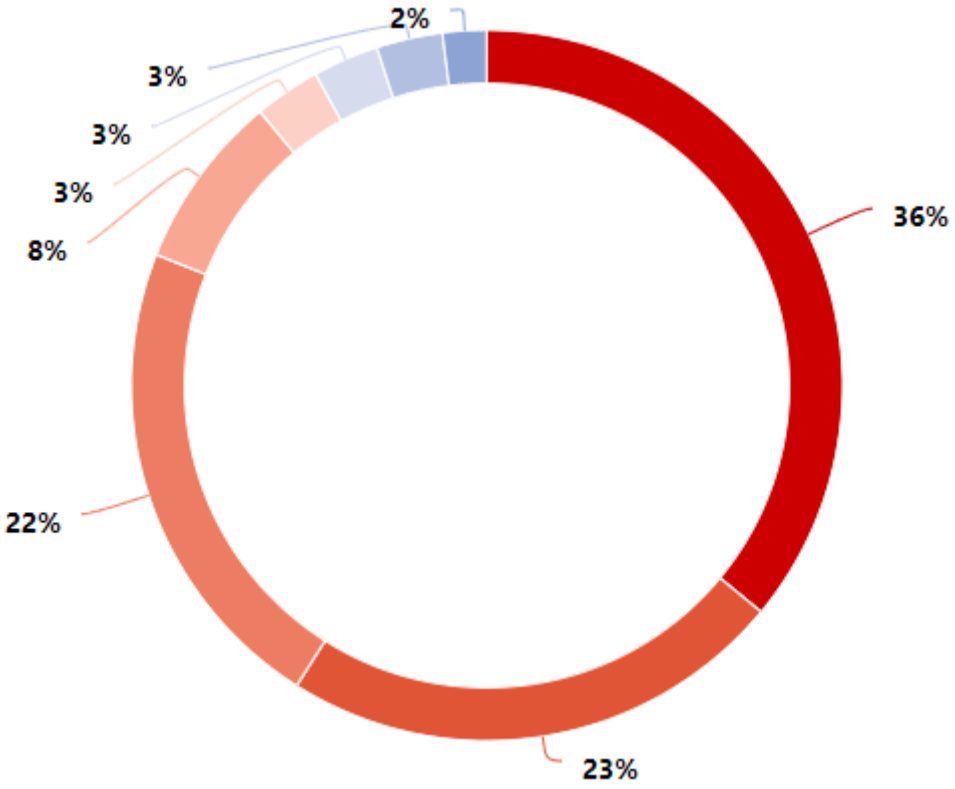

Рисунок 1.2 – Типи вкрадених даних (при атаці на організації)

Де: 36% - персональні дані, 23% - облікові записи, 22% - комерційні таємниці, 8% - медична інформація, 3% - база даних клієнтів, 3% - переписки, 3% - дані платіжних карт,2% - інша інформація.

Звичайно, це не всі мотиви, якими керують сучасні хакери, щоб керувати своєю діяльністю. Іноді буває важко визначити мотив у цілому. Буває, що причина нападу виявляється зовсім екзотичною – наприклад, екологічні проблеми. Або дуже банальні – заздрість, ревнощі. Крім того, відсоток атак – це звичайний комп'ютерний вандалізм. Експерти з комп'ютерної безпеки називають це Destruction Wish. Навіть професійним психологам часто буває важко зрозуміти, чому звичайна людина «на вічі» починає видаляти файли та каталоги на чужих комп'ютерах, розсилати поштові бомби, записувати та поширювати віруси та навіть фізично, наприклад, мережеві пристрої в пошкодження.

1.3 Advanced Persistent Threat

Фахівці з інформаційної безпеки по-різному тлумачать термін Advanced Persistent Threat (APT). Варіанти включають: «розширені постійні загрози»; «Розширені», «Розроблені», «Комплексні» та «Цільові» загрози. Експерти Positive Technologies визначають APT як добре організовану, ретельно сплановану кібератаку, спрямовану на конкретну компанію або цілу галузь. Зловмисник отримує несанкціонований доступ до мережі, оселяється в інфраструктурі і тривалий час залишається непоміченим. Ці атаки зазвичай підтримують групи APT, які мають значні фінансові ресурси та технічні навички.

Масові кібератаки спрямовані на глобальне поширення шкідливого програмного забезпечення, в основному вражають окремих осіб і не вимагають тривалої підготовки та значних фінансових вкладень. Кіберзлочинці не враховують галузь і розміри компанії при плануванні таких атак, не створюють портрет жертви, а використовують для їх реалізації готові інструменти, дешевші за цілеспрямовані атаки.

З іншого боку, цілеспрямована атака завжди спрямована проти конкретної компанії, комп'ютерної мережі чи комп'ютера окремого працівника. Такі атаки завжди ретельно продумані, розтягнуті в часі і реалізовані в кілька етапів. Згідно з дослідженням Verizon, зловмиснику потрібно кілька хвилин, щоб проникнути в інфраструктуру, а для виявлення атаки потрібні тижні або навіть місяці.

І торгові компанії, і державні установи зазнають нападів з боку APT-груп. За даними Positive Technologies, основними категоріями жертв цілеспрямованих атак є державні установи, промислові компанії, фінансова галузь, паливно-енергетичний комплекс. Аерокосмічна промисловість, IT-компанії, підприємства військового оборонного комплексу та наукові установи також піддаються великому ризику.

Як правило, зловмисники полюють за секретними стратегічними розробками, платіжною інформацією, персональною інформацією – будь-якою інформацією, яку можна вигідно продати, обміняти або використати.

Атакою клієнтів можуть стати конкуруючі компанії та спеціалізовані служби. Атаки зазвичай здійснюють групи APT - групи професійних хакерів, які фінансуються зацікавленою стороною. Вони самі виготовляють інструменти для злочинів або купують їх у даркнеті.

Найімовірніше в тому випадку, якщо кіберзлочинці отримають дані для доступу до банківських рахунків і проведення незаконних операцій. Це особливо актуально для фінансових установ.

Якщо конфіденційна інформація потрапляє в руки зловмисників, це може зашкодити іміджу компанії та спровокувати відтік клієнтів

Цілеспрямовані атаки часто порушують стабільність бізнес-процесів. Компанії потрібен час на дослідження та ресурси, щоб повернути бізнес у правильний шлях (рис. 1.3).

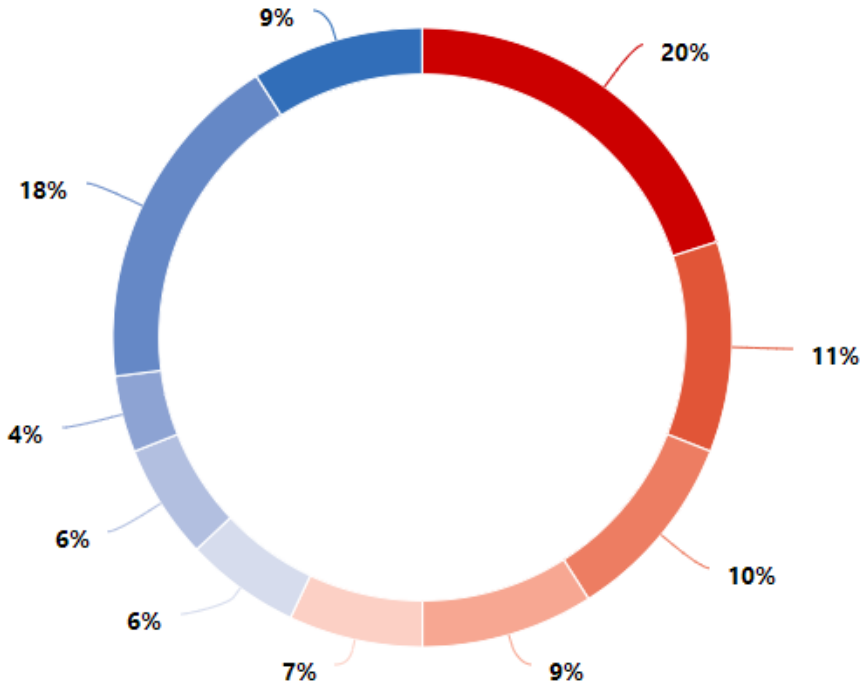

Рисунок 1.3 – Категорії жертв організацій

Де: 20% - держустанови, 11% - промисловість, 10% - медичні заклади, 9% - Наука та освіта, 6% - IT-компанії, 6%- сфера обслуговування, 4% - фінансові організації, 18% - інші, 9% - без зв’язку к галуззю.

Іноді кінцевою метою є саботаж: наприклад, цілеспрямовані атаки відрізняються в промисловості та в паливно-енергетичному комплексі, де ризик простою є більш небезпечним, ніж втрата даних.

Окрім прямого збитку, компанії також зазнають непрямих втрат, які є результатом необхідності будувати захист від цілеспрямованих атак. Необхідно покращити роботу існуючої системи інформаційної безпеки, а для цього необхідно придбати нове програмне забезпечення, переглянути бізнес-процеси, залучити нових спеціалістів з кібербезпеки та підвищити рівень обізнаності працівників щодо соціальної інженерії.

1.4 Методи атак (частка атак) на організації та приватних осіб

Атака на інформаційну систему - це дія або послідовність взаємопов'язаних дій зловмисника, що призводить до реалізації загрози шляхом використання слабких місць цієї інформаційної системи.

Фішинг. Його мета — отримати інформацію від користувачів (паролі, номери кредитних карток тощо) або гроші. Ця техніка розрахована не на одного користувача, а на багатьох. Наприклад, листи нібито розсилає техпідтримка всім відомим клієнтам банку.

Зазвичай у листах міститься прохання надіслати пароль на обліковий запис, нібито через технічні роботи. Такі листи зазвичай пишуться дуже достовірно, що може залучити довірливих користувачів.

Рекомендації: Не довіряйте підозрюваному, не передавайте свої дані третім особам. Адміністраторам не потрібно знати ваш пароль, якщо він

використовується для доступу до їхнього сервера. Ви повністю контролюєте сервер і можете переглядати або змінювати пароль самостійно.

Соціальна інженерія - це не технічна, а психологічна техніка. З даними, отриманими під час інвентаризації, зловмисник від імені адміністратора може зателефонувати будь-якому користувачеві (наприклад, мережу компанії) і спробувати його використати, наприклад. В. щоб дізнатися пароль.

Це стає можливим, коли у великих мережах користувачі не знають всіх співробітників і, перш за все, не завжди можуть точно ідентифікувати їх по телефону. Крім того, використовуються складні психологічні прийоми, завдяки чому шанси на успіх значно збільшуються.

Рекомендації: якщо дійсно є потреба, будь ласка, надайте необхідні дані особисто. Після того, як ви записали пароль на папері, не залишайте його ніде, знищуйте його, а не просто викидайте в смітник.

DoS (відмова в обслуговуванні). Це не сама по собі атака, а результат нападу. Використовується для деактивації системи або окремих програм. Для цього зломщик спеціальним чином відправляє запит до програми, згідно з яким вона більше не працює. Щоб повернути програму в робочий стан, потрібен перезапуск.

UDP-бомба - зломщик відправляє в систему UDP-пакет з некоректними полями службових даних. Дані можуть бути пошкоджені будь-яким чином (наприклад, неправильна довжина полів, структура). Це може призвести до аварії. Рекомендації: Оновіть програмне забезпечення.

Поштові бомбардування. Якщо атакуваний комп’ютер має поштовий сервер, на нього надсилається багато поштових повідомлень, щоб вимкнути його.

Крім того, такі повідомлення зберігаються на жорсткому диску сервера і можуть заповнювати його, що може призвести до DoS. Звичайно, зараз ця атака - це більше історія, але в деяких випадках її все ще можна використовувати. Рекомендації: Грамотно налаштуйте поштовий сервер.

Sniffing. Якщо в мережі замість комутаторів встановлені концентратори, отримані пакети відправляються на всі комп’ютери мережі, а потім комп’ютери визначають, який пакет для них чи ні.

Якщо зловмисник отримує доступ до комп’ютера, інтегрованого в таку мережу, або якщо він отримує прямий доступ до мережі, стає доступною вся інформація, що передається в сегменті мережі, включаючи паролі.

Зловмисник просто переведе мережеву карту в режим прослуховування і прийме всі пакети, незалежно від того, чи призначені вони для нього.

Рекомендації: використовуйте комутатори замість концентраторів, шифруйте трафік.

IP Hijack. Якщо є фізичний доступ до мережі, зловмисник може «перерізати» мережевий кабель і виступити посередником у передачі пакетів і таким чином підслухати весь трафік між двома комп’ютерами. Це дуже громіздкий спосіб, який часто не виправданий, за винятком випадків, коли неможливо застосувати інший спосіб.

Такий запис незручний сам по собі, хоча є пристрої, які дещо спрощують це завдання, зокрема контролюють нумерацію пакетів, щоб уникнути помилки та можливого виявлення вторгнення в канал.

Рекомендації: переконайтеся, що є кабельний доступ у кабельні канали. Шифруйте трафік.

Фіктивний DNS-сервер Якщо мережеві параметри встановлено на автоматичний режим, коли комп'ютер підключений до мережі, він «запитує», хто буде його DNS-сервером, на який потім надсилає запити DNS.

Маючи фізичний доступ до мережі, зловмисник може перехопити такий широкомовний запит і відповісти, що його комп’ютер буде DNS-сервером.

Тоді він може відправити зраджену жертву будь-яким маршрутом. Наприклад, якщо жертва хоче зайти на сайт банку і переказати гроші, зловмисник може відправити їх на свій комп’ютер, де підроблено форму для введення пароля. Після цього пароль належить зломщику.

Досить складний метод, оскільки зловмисник повинен відповісти жертві перед DNS-сервером.

Рекомендації: якщо можливо, обмежте зовнішній доступ до мережі.

Підробка IP-адрес (спуфінг або підробка IP-адрес). Зловмисник замінює свій справжній IP на підроблений. Це необхідно, якщо доступ до ресурсу мають лише певні IP-адреси. Зловмиснику доведеться змінити свою реальну IP-адресу на «привілейований» або «довірений», щоб отримати доступ. Цей метод можна використовувати й іншими способами.

Після того, як два комп'ютери встановили з'єднання шляхом перевірки паролів, зловмисник може перевантажити мережеві ресурси жертви спеціально згенерованими пакетами. Таким чином він може перенаправляти трафік собі і таким чином обійти процес аутентифікації.

Рекомендації: Загроза зменшується за рахунок зменшення часу відповіді пакету з встановленими прапорами SYN і ACK і збільшенням максимальної кількості запитів SYN для встановлення з'єднання в черзі (tcp_max_backlog). Ви також можете використовувати файли cookie SYN.

Уразливості програмного забезпечення. Використання помилок у програмному забезпеченні. Ефект може бути різним. Від отримання несуттєвої інформації до повного контролю над системою. Атаки програмних помилок є найпопулярнішими за всі часи (рис. 1.4).

Старі помилки виправляються новими версіями, але нові помилки з'являються в нових версіях, які можна використовувати повторно. Найпоширеніша проблема, відома звичайному користувачеві. Суть полягає в запровадженні шкідливої програми в комп'ютер користувача. Наслідки можуть бути різними і залежать від типу вірусу, що заражає комп'ютер.

Але загалом – від крадіжки інформації, розсилки спаму, організації DDoS-атак до повного контролю над комп'ютером. Крім файлу, прикріпленого до листа, деякі прогалини безпеки в операційній системі можуть стати причиною проникнення вірусів на комп'ютер.

Рекомендації: Використовуйте антивірусне програмне забезпечення. Використовуйте спеціальні антивіруси проти шкідливих програм, наприклад Ad-Aware, SpyBot, XSpy.

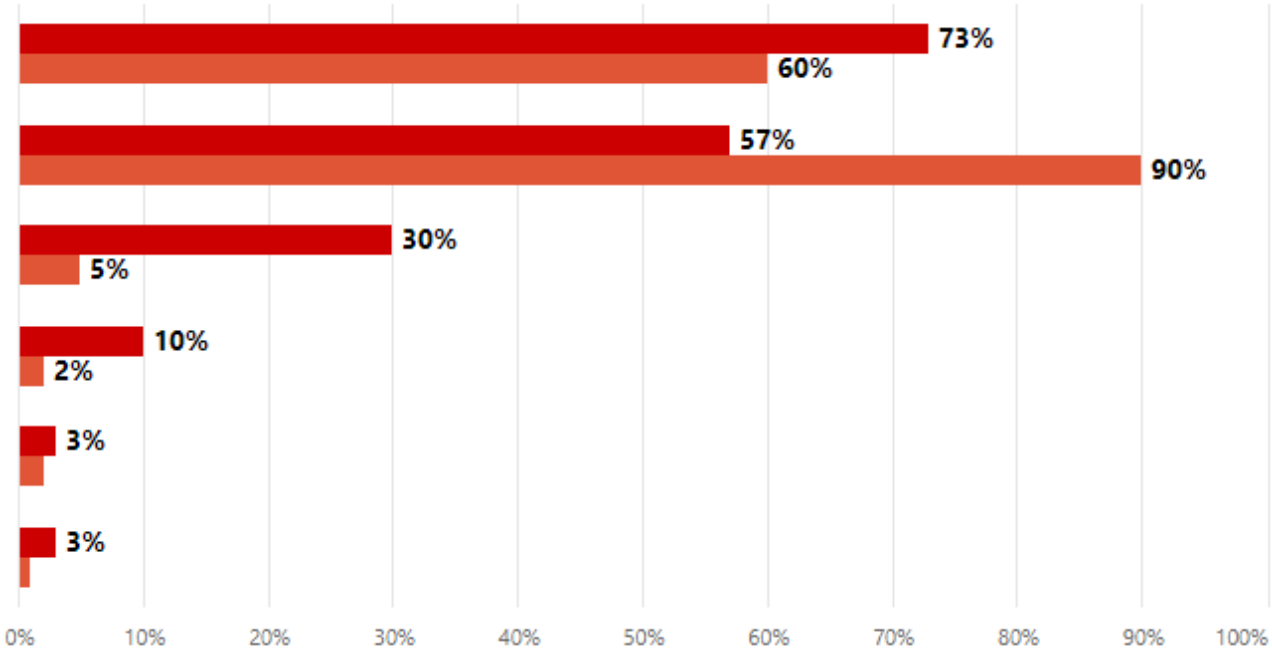

Рисунок 1.4 – Методи атак (частка атак) на організації та приватних осіб

Де: 73% та 60% - використанням ВПЗ, 57% та 90% - соціальна інженерія, 30% та 5% - хакінг, 10% та 2% - експлуатація веб-вразливостей, 3% та 2% - підбір облікових записів, 3% та 1% - інші.

Частка атак зловмисного програмного забезпечення на компанії зросла на 15 процентних пунктів у порівнянні з першим кварталом 2021 року і становить 73%. Лідируючі позиції серед шкідливих програм, що використовуються при атаках на бізнес, як і раніше займають програми-вимагачі. До речі, за квартал частка атак з такими програмами зросла з 63% до 69%. У порівнянні з першим кварталом частка атак завантажувачів зросла більш ніж вдвічі(рис. 1.5).

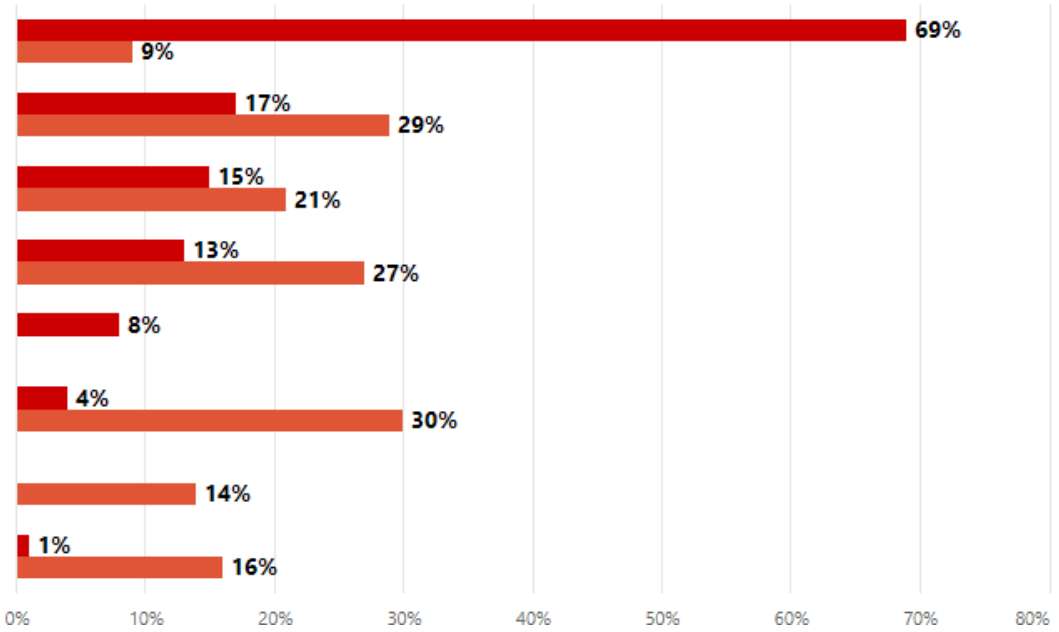

Рисунок 1.5 – Типи шкідливого ПЗ (частка атак з використанням ВПЗ) на організації та приватних осіб

Де: 69% та 9% - шифрувальники, 17% та 29% - ВПЗ для віддаленого доступу, 15% та 21% - завантажувач, 13% та 27% - шпигунське ПЗ, 8% - майнер, 4% та 30% - банківський троян, 14% - рекламне ПЗ, 1% та 16% -інші.

1.5 Проникнення в корпоративну мережу

Найпоширеніших уразливости мережевого периметра промислових компаній є недоліки конфігурації займають 7 з 10 рядків.

Наявність зовнішньому інтерфейсів адміністрування серверів CIS та віддаленого доступу до СУБД, а також узагальнене використання словника та стандартних паролів привілейованих користувачів дозволяє за один крок отримати повний контроль. через веб-додатки та сервери, отримувати доступ до баз даних і файлів і розробляти атаку на інші ресурси. Важливі дані, що зберігаються у відкритому доступі, такі як облікові записи, вихідний код веб-додатків, особисті дані користувачів, можуть бути використані в атаках.

Уразливості в коді веб-додатків увійшли в десятку найпоширеніших уразливостей периметра мережі.

Використання таких уразливостей, як віддалене виконання команд і довільне завантаження файлів, дозволяє перетинати периметр промислового підприємства, якщо веб-додаток знаходиться на сервері, підключеному до локальної мережі.

Оскільки веб-додатки є невід'ємною частиною бізнес-інформаційної системи промислових організацій, їх безпеці приділяється недостатньо уваги. Згідно з дослідженнями, майже кожне друге веб-додаток (43%) на периметрі корпоративної інформаційної системи промислових компаній характеризується надзвичайно низьким рівнем безпеки.

Високий рівень ризику характерний для кожної другої вразливості при оцінці найбільш поширених вразливостей периметра мережі промислового підприємства.

Застарілі версії програмного забезпечення (наприклад, веб-сервери, операційні системи, прикладні системи) часто містять критичні вразливості, якими може скористатися зловмисник, щоб отримати контроль над ресурсами. Для багатьох із цих вразливостей існують публічні дії. Не менш небезпечними можуть бути й помилки конфігурації: надмірні привілеї СУБД або веб-сервера дають можливість у разі доступу до них виконувати команди ОС на сервері з максимальними привілеями. Навіть обмежені привілеї в серверній ОС, яка розташована по периметру мережі, але також має інтернет-інтерфейс, дозволяють зловмиснику розробити вектор атаки на внутрішні ресурси компанії.

Переважна більшість успішних векторів атак по периметру для промислових підприємств покладається на використання вразливостей у веб-додатках. Зокрема, такі вразливості, як SQL Injection, Arbitrary File Upload і Remote Command Execution, були використані для перетину периметра.

Використання словникових паролів для доступу до систем адміністрування веб-серверів або для віддаленого підключення за допомогою протоколів керування виявлено майже у всіх компаніях, і в третині з них це дозволило розробити вектор атаки перед доступом до локальної мережі.

Не секрет, що застарілі версії CMS і веб-серверів містять багато вразливостей, для яких в Інтернеті вже є розроблені експлойти. Зловмиснику нескладно використовувати їх і взяти під контроль сервер.

Помилки конфігурації системи, наприклад, неправильне розмежування прав доступу для користувачів веб-додатків, також можуть призвести до компрометації сервера в межах периметра інформаційної системи компанії.

У рамок тестів на проникнення експертами оцінювалася складність вектора проникнення в локальну мережу з Інтернету, враховуючи як навички зловмисника, так і спеціальні інструменти, необхідні для атаки, а також наявність загальнодоступні експлойти, наявність додаткових умов для успішної атаки та інші фактори.

У більшості випадків атака вважалася простою, наприклад, якщо для отримання контролю над сервером достатньо було обійти фільтрацію розширень під час завантаження файлів через веб-додаток, або якщо використовувався доступний для всіх експлойт, код якого мав пройти незначні модифікації для адаптації до певної системи. Тривіальний рівень складності призначався у випадках, коли атака не вимагала жодних подальших дій, наприклад, у випадку стандартного пароля для доступа до системи адміністрування веб-сервера з подальшим використанням вбудованих системних функцій для виконання команд на сервер.

Структура бізнесу різна в кожній галузі, і, звичайно, кожна організація має свій власний підхід до сегментації та захисту мережі. Однак помилки впровадження та хибні уявлення про адміністрування подібні в багатьох компаніях. Щоб наочно показати ці проблеми ІС, ми спробували об’єднати основні принципи побудови захищеної мережі та реалізувати їх в єдину масштабовану схему. Такий підхід до побудови мережі не зустрічався на жодному з досліджуваних об’єктів, однак, він суттєво ускладнює потенційний вектор атаки та значно знижує ризик скомпрометації ІКС.

Для побудови структурної схеми підрозділу мереж визначають такі основні вимоги розглянемо:

– ІС має бути строго відокремлена від інформаційної системи компанії та зовнішніх мереж, особливо Інтернет;

– інформація про технологічний процес і стан обладнання повинна передаватися через спеціальний шлюз. Найбезпечніша реалізація – через DMZ, дотримуючись рекомендацій NIST 800-82 (розділ 5.5.5). Передача команд управління від інформаційної системи компанії до компонентів ICS або до вузлів шлюзу повинна бути заборонена;

– збір інформації, що надходить від шлюзів різних промислових об'єктів (вони можуть бути територіально розділені), здійснюється в автоматизованій системі управління, складові частини якої виділяються в окремий сегмент. У цьому ж сегменті можуть бути розташовані робочі місця аналітиків і менеджерів, які обробляють зібрані дані;

– контроль технологічних процесів, адміністрування та безпеки інформації в транспортному засобі здійснюється тільки спеціальними підрозділами всередині транспортного засобу.

На жаль, на практиці багато з перерахованих правил не дотримуються або дотримуються формально. Це дає можливість в рамках внутрішніх тестів на проникнення виявити різні вектори атак на транспортний засіб.

Типову атаку, яка дозволяє зловмиснику, який працює з сегменту локальної мережі компанії, проникнути в промислову мережу компанії і порушити технологічний процес, можна розбити на три основні етапи:

– отримання та підвищення привілеїв операційної системи на вузлах інформаційної системи компанії;

– розробка атаки та консолідація в інформаційній системі компанії;

– отримання доступу до критичних систем і розробка атак.

Кожен крок може бути реалізований по-різному, але правопорушник повинен діяти, з одного боку, максимально ефективно, з іншого -максимально

стримано. Таким чином, в рамках тестів на проникнення експерти перевіряють можливість реалізації максимальної кількості сценаріїв атак і оцінюють складність і ймовірність їх реалізації.

Далі кожен етап атаки буде детально розглянуто. Буде представлена статистика щодо впровадження окремих методів атаки, а також статистика щодо виявлення вразливостей та вразливостей безпеки, використаних під час атаки. Для наочності буде наведено функціональні схеми типових векторів атаки.

Отримання та підвищення привілеїв операційної системи на вузлах інформаційної системи компанії.

У разі відсутності привілеїв в інформаційній системі компанії (наприклад, якщо зловмисник не є співробітником або субпідрядником організації), зловмисник повинен отримати доступ до мережі компанії. Для цього він може використовувати доступні мережеві розетки, гостьовий Wi-Fi або здійснити інтернет-атаку.

Після отримання доступу до інформаційної системи компанії основним завданням зловмисника є отримання та збільшення локальних привілеїв на серверах і робочих станціях співробітників, а також збір інформації про топологію мережі, використовувані пристрої та програмне забезпечення.

Розробка атаки та консолідація в інформаційній системі компанії.

Отримавши максимум локальних привілеїв на одному або кількох вузлах інформаційної системи компанії, зловмисник повинен розробити атаку на інші доступні ресурси, щоб захистити його в інформаційній системі компанії та визначити пристрої, з яких можна здійснити атаку. отримати доступ до транспортного засобу.

Розробка атаки на корпоративну мережу здійснюється з використанням уразливостей програмного забезпечення, операційних систем і веб-додатків, лазівок сегментації мережі та аутентифікації користувачів. Додатково може використовуватися інформація, отримана з загальнодоступного сховища файлів (наприклад, облікові дані або файли конфігурації обладнання). Мета

правопорушника – отримати максимальні привілеї на місцевості та визначити точки входу в транспортний засіб, зібрати інформацію.

Отримання доступу до критичних систем і розробка атак.

Як правило, результатом другого кроку є отримання привілеїв адміністратора домену та багатьох привілейованих облікових записів співробітників в організації. Зловмисник має додаткові знання про бізнес-процеси та системи, що використовуються, налаштування обладнання та іншу інформацію, яка може бути використана для проникнення в транспортний засіб. Зловмисник може використовувати отримані привілеї та інформацію, щоб ідентифікувати існуючі канали підключення до автомобіля. Крім того, зловмисник може використовувати отримані привілеї для зміни конфігурації мережевих пристроїв, щоб побудувати власний канал у транспортному засобі.

Початковий етап атаки залежить від можливості зловмисника отримати доступ до ресурсів локальної мережі та рівня привілеїв на ці ресурси. Як правило, у разі атак зловмисника, який не має привілеїв у корпоративних системах підприємства, складність атаки досить висока, оскільки для підключення до мережі він повинен отримати доступ до розетки, розташованої всередині будівлі, доступ до якого обмежений для відвідувачів, які не мають зарплати. Але деякі помилки конфігурації мережі можуть спростити вектор проникнення.

Якщо інсайдером є, наприклад, співробітник компанії, підприємець, партнер або навіть двірник, ймовірність вдалого компромісу критичних ресурсів значно зростає. Саме внутрішній зловмисник, що працює з сегмента користувачів інформаційної системи компанії, є найбільш вірогідним джерелом атак на об’єкти транспортних засобів.

На промислових об’єктах повсюдно зустрічаються застарілі версії операційних систем і програмного забезпечення. Це тому, що часто просто неможливо встановлювати оновлення на регулярній основі, не порушуючи робочого процесу, а в деяких системах встановлення оновлень для певних компонентів може вплинути на їх сумісність з іншими. Останнє може слугувати

переконливим аргументом при оцінці ризиків для технологічного сегмента, який має бути жорстко відокремлений від інших зовнішніх мереж, у тому числі для подолання цих прогалин у безпеці. Для корпоративної мережі, яка, крім усього іншого, має доступ до Інтернету, використання застарілих версій програмного забезпечення та ОС неприпустимо (рис. 1.6).

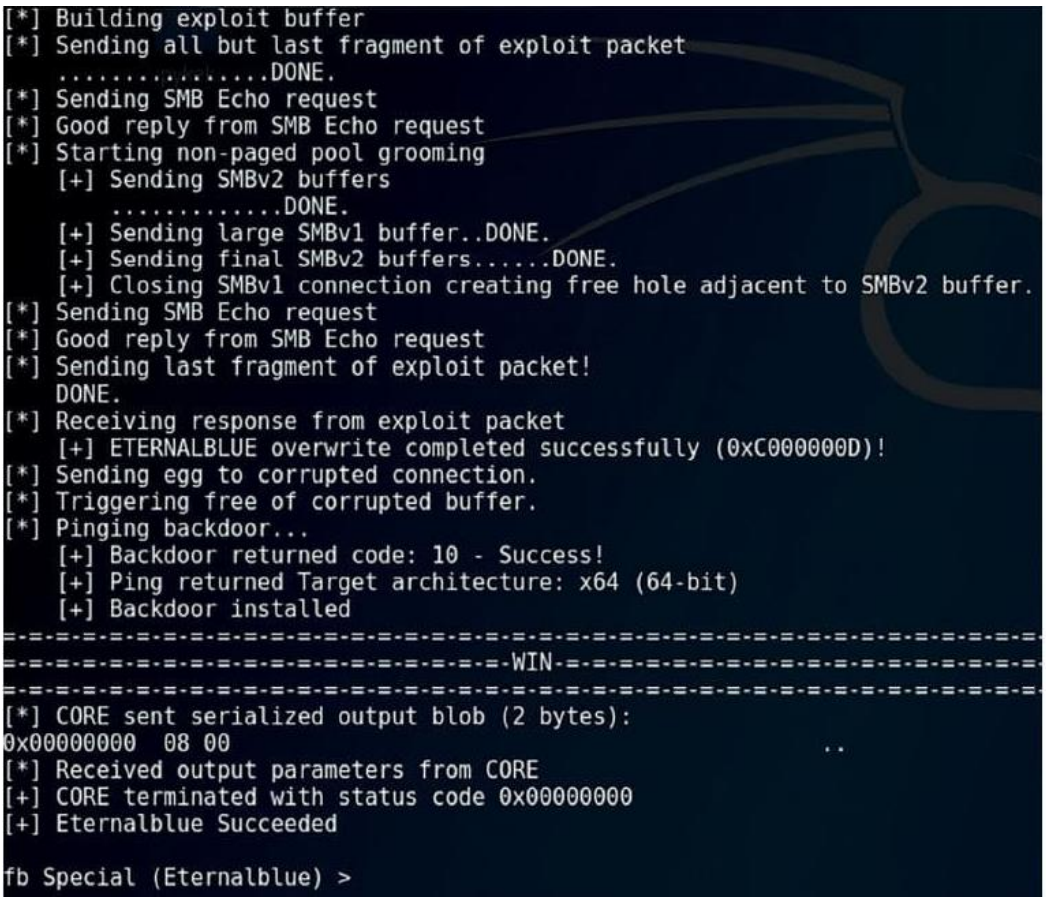

Рисунок 1.6 – Приклад SMB атак.

Резонансними прикладами атак із використанням таких уразливостей є спалахи програм-вимагачів WannaCry та NotPetya, які відбулися у 2017 році та вразили багато організацій у всьому світі, у тому числі промислові. У рамках цих кампаній кіберзлочинці активно використовували вразливість MS17-010 у Windows. Відповідний експлойт EternalBlue був випущений через місяць після виходу виправлення для усунення вразливості.

Привілеї локального адміністратора на комп’ютерах під керуванням Windows дозволяють зловмиснику або запустити спеціальну утиліту для отримання облікових даних користувача з пам’яті операційної системи (наприклад, mimikatz), або створити копію .exe і вже на своєму ноутбуці за допомогою тієї ж утиліти для зчитування паролів або хешів паролів від користувачів операційної системи. Ця атака та методи обходу засобів захисту під час її виконання вже були детально показані в нашому дослідженні типових сценаріїв атак на інформаційні системи компанії, спостерігаємо лише те, що у всіх перевірених нами компаніях вона була виявлена можливо здійснити атаку зі 100% успіхом навіть у випадку антивірусних засобів на серверах і робочих станціях. Це пов’язано з використанням старих версій ОС, для яких не існує ефективного методу захисту.

Всі ці фактори в тій чи іншій мірі знижують рівень безпеки PCSA. Сьогодні промислові компанії не готові протистояти цілеспрямованим кібератакам. Важливо розуміти, що одиничний IT-інцидент на промисловому об’єкті може призвести до непоправних наслідків – нещасних випадків та загибелі людей. Тому необхідно вживати превентивних захисних заходів, виявляти та усувати вразливі місця, а також інформувати працівників щодо питань інформаційної безпеки.

2 ПРОТОКОЛИ ЗАХИСТУ

Безпека мережі - це не мета, це процес! Колесо безпеки Cisco добре описує еволюцію системи безпеки (рис. 2.1).

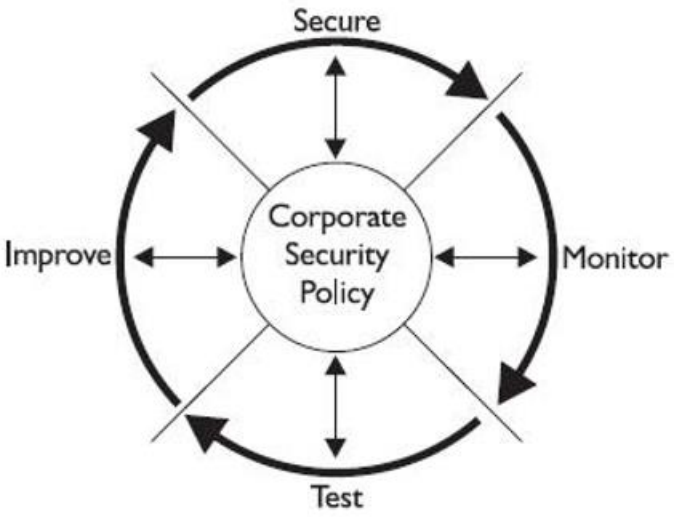

Рисунок 2.1 – Колесо безпеки Cisco

Ця презентація заснована на корпоративній політиці безпеки, яка базується на чотирьох компонентах: захист, моніторинг, тестування, покращення [8].

Є три основні способи забезпечення інформаційна безпека. Організація інформаційної безпеки може бути досягнуто шляхом використання організаційних матеріалів, засоби захисту інформації (технічні) або програмні методи. Кращий ефективність буде досягнута у разі застосування комплексного захисту з перерахованих вище методів.

Перераховані вище способи можуть бути реалізується різними засобами:

– захистіть периметр інформаційної системи шляхом застосування створюються організаційні засоби;

– охоронно-пожежна сигналізація;

– цифрові системи відеоспостереження;

– системи контролю та управління доступом (СКУД) тощо.

Захист інформації від витоку через технічні канали зв'язку забезпечується за допомогою таких засобів і заходів:

– використання екранованого кабелю та кабелю та кабелі в броньованих конструкціях;

– встановлення високочастотних фільтрів на лініях зв'язку;

– будівництво екранованих приміщень («капсули»);

– використання бронетехніки;

– встановлення систем активного шумового контролю;

– створення контрольованих зон тощо.

Засоби захисту обладнання включають різні електронні пристрої, електромеханічні, електрооптичні прилади.

В даний час найбільш поширеними є наступний матеріал:

– спеціальні регістри для зберігання інформації безпеки: паролів, ідентифікаційні коди, штампи або рівні секретності;

– прилади для вимірювання індивідуальних особливостей людини (голос, відбитки пальців) з метою ідентифікації;

– схеми переривання передачі інформації в лінії зв'язку для того, щоб періодично перевіряти адресу передачі даних;

– пристрої шифрування інформації (криптографічні методи) та інші.

2.1 Антивірусне програмне забезпечення

Це програма для виявлення комп'ютерних вірусів, небажані програми (вважаються шкідливими) та відновлення файли, заражені (змінені) такими програмами, а також профілактика - запобігання зараженню (модифікації) файлів або операційної системи шкідливий код.

Класифікація антивірусів за принципом їх дії:

– сканери. Принцип їх роботи полягає в пошуку файлів, пам'яті і вірус унікальний програмний код завантажувальних секторів - вірусний маски. Вірусні

маски (описи) містяться в антивірусній базі, і якщо сканер зустріне програмний код, який відповідає будь-якому з цих описів, потім він видає повідомлення про виявлення вірус;

– аудитори. Запам'ятати стан комп'ютера, відстежувати зміни файлову систему та повідомляти про важливі або підозрілі зміни користувач;

– монітори. Це тип сканера, який знаходяться в пам’яті комп’ютера та виконують автоматичну перевірку всі файли, які використовуються в режимі реального часу. Сучасний монітори перевіряють при відкриванні та закриванні програми;

– вакцини (імунізатори). Вони діляться на два типи: вакцини, повідомляти про інфекцію та вакцини, що блокують зараження будь-яким типом вірусу;

Класифікація антивірусів за функціональним призначенням:

– антишпигунське програмне забезпечення. Розроблена антивірусна програма щоб виявити та видалити шпигунське програмне забезпечення з вашого комп’ютера користувач;

– онлайн-сканер. Антивірусний засіб виявлення та видалення вірус із файлової системи персонального комп'ютера, підключеного до інтернет. Їх головна перевага – відсутність необхідність встановлення програми. Мінусом є те сканер виявляє лише віруси, які вже проникли в систему і ще ні здатний захистити ваш комп'ютер від майбутнього зараження;

– брандмауер. Це програма, яка забезпечує а робота комп'ютера в мережі, що дозволяє блокувати небажаних людей мережевий трафік, а також забезпечує невидимість комп'ютера в мережі, со щоб запобігти нападам піратів;

– комплексний захист. Програмні пакети, які забезпечують всі перераховані вище засоби захисту комп’ютера плюс додаткові функціональні компоненти. Може містити антивірус, брандмауер, антишпигунське програмне забезпечення, захист від фішингу, антиспам, інструмент резервне копіювання даних;

Кожному існуючому вірусу присвоюється унікальний фрагмент коду, так званий підпис. Цей фрагмент коду зберігається в базі данихантивірус, і якщо такий фрагмент коду знайдено у файлі, то такий файл ідентифікується як відповідний вірус. Після знаходження підозрілий файл, залежно від налаштувань, встановлених на ПК антивіруса, користувач отримує або повідомлення про право вибору Долю цього файлу або антивірусної програми вирішує сама його. Однак для бази сигнатур антивірусної програми бути з'явився унікальний вірусний код, цей вірус повинен отримати для аналізу вірусними аналітиками компанії-розробника антивірусів розташування. Це довгий шлях. є тисячі нові різновиди вірусів, а антивірусна програма повинна бути якісною захистити програмне забезпечення. Щоб вирішити таку проблему, з’являйтеся регулярно оновлення для антивіруса, а також деяких антивірусів програми мають таку властивість, як евристичний аналіз.

Евристичний аналіз працює інакше, ніж наведений вище база даних підписів. Він сканує вміст файлу і не знаходить ознака і послідовність операцій, характерних для вірусів. Тому антивірусна програма має можливість виявляти віруси, які ще не були розглянуті вірусними аналітиками. більшість ідеальний евристичний алгоритм сканування використовує антивірус, та це надійніше.

При виборі антивірусного програмного забезпечення користувачі керуються вимоги, які їх цікавлять.

Критерії оцінки антивіруса:

– кількість відомих вірусів;

– швидкість реакції на появу нових вірусів;

– ступінь використання IT-ресурсів;

– наявність евристичного аналізу;

– правильне лікування вірусів;

– наявність антивірусного модуля, який працює в режимі реального часу.

2.2 Брандмауери або міжмережові екрани

Він є важливим елементом системи безпеки локальних мереж або персональні комп'ютери, підключені до глобальної мережі.

Для збільшення необхідно використовувати брандмауер комп’ютерна безпека шляхом обмеження інформації від інші комп’ютери, відстежуючи будь-які несанкціоновані дії програми та програми, які намагаються отримати доступ до інформації локальні ресурси комп’ютера.

Для боротьби з несанкціонованими брандмауерами брандмауер повинен бути розташований між захищеною мережею і потенційним зловмисником. З організаційної точки зору щит є частиною захищеної мережі. Брандмауер не симетричний. Для цього встановіть окремо параметри, що обмежують доступ із внутрішньої мережі до зовнішньої мережі та навпаки. Брандмауер повинен бути сумісним із протоколом обмін інформацією, що становить основу внутрішнього та зовнішнього обміну мережі. Якщо ці протоколи відрізняються, брандмауер повинен підтримує багатопротокольний режим.

Брандмауери контролюють мережевий трафік, що проходить всередині локальна мережа, дозволить вам пройти лише через мережеве з’єднання дозволив трафік, таким чином керуючи мережевим зв’язком між комп’ютерами глобальної та локальної мережі. Брандмауери дозволяють приховати IP-адреси хостів всередині локальної мережі за допомогою операції, називається транзакцією трансляції мережевої адреси (NAT). Маскування IP-адреси стає невидимим для зовнішнього світу користувачів, які, наприклад, надсилають повідомлення електронної пошти внутрішній користувач спрямовується на поштовий шлюз, який пересилає його одержувачу.

Брандмауери дозволяють контролювати доступ користувачів мережі до різноманітні мережеві послуги. Це завдання вирішується шляхом налаштування брандмауер, до якого ви можете дозволити або заблокувати доступ окрема служба локальної мережі з використанням списків контролю доступу (Список

контролю доступу). ACL забезпечують гнучкість управління доступом. З їх допомогою ви можете дозволити доступ до послуг і відмовити в доступі до всіх інших послуг, або, навпаки, заблокувати доступ до певних служб і дозволити доступ до всіх інші послуги. Добре налаштовані брандмауери – це непросто блокувати несанкціоновані запити від зовнішніх комп'ютерів, але і спробуйте ідентифікувати запитувачів з а інформувати користувача-адміністратора системи про будь-які такі спроби запити.

Брандмауери складаються з набору програмного та апаратного забезпечення компоненти, до складу яких входять наступні.

1. Бастіонний хост. Це захищений комп'ютер операційної системи, підключена до локальної та глобальної мережі. На бастіоні всі інші компоненти брандмауера встановлені на комп'ютері та необхідні послуги, такі як Telnet, DNS, FTP, SNMP та інструменти персоналізована аутентифікація.

2. Маршрутизатор з фільтрацією пакетів. Звичайний роутер просто пересилає вхідні IP-пакети на вказану адресу. Виконує маршрутизатор фільтрації пакетів функція перевірки вхідних IP-пакетів. Маршрутизатори з фільтрацію пакетів іноді називають безпечними маршрутизаторами. Захищені маршрутизатори не перевіряють вміст пакетів, але мають обробляти лише інформацію заголовка пакета, перевіряти IP-адреси джерело і призначення, використовувані протоколи, послуги, порти та інші відомості, зазначені в ДМЗ.

3. Шлюзи додатків (application gateways). Використовується на bastion host і обмежити зв'язки для окремих осіб додатків. Для цього використовуються посередницькі послуги, які встановлюється на шлюзі окремо для кожної програми, яка мережеве спілкування через брандмауер дозволено. Тільки ці мережі служби, для яких встановлені проксі-сервіси, можуть отримувати і надсилати мережевий трафік через шлюзи програм, а посередницькі послуги можна налаштувати так, щоб дозволити доступ лише до обмежений набір інструментів застосування. Таким чином, шлюзи програми значно покращити можливість створення такої політики безпеки, який забезпечить аутентифікацію

та обслуговування користувачів мережі журнал запису. Прикладом шлюзу прикладного рівня є проксі-сервер, який обробляє мережевий трафік і працює Аутентифікація користувача.

4. Шлюзи каналів. Підключіть мережевий комп'ютер до портів TCP / IP бастіонний господар. Вони не виконують жодної перевірки мережевого трафіку та використовуються для пересилання довірених вихідних повідомлень внутрішні користувачі. Дозволяє захистити вашу мережу від вторгнень і в той же час час для прискорення системи.

Брандмауери фільтрують пакети, перевіряючи заголовки вхідних пакетів для їх задоволення певним критерії, визначені за допомогою правил фільтрації пакетів. Фільтри наносяться на пакети зсередини і зовні. локальної мережі, а фільтр працює асиметрично, по-різному обробляти вхідні та вихідні пакети. Це щоб відфільтрувати записи та вихідні пакети повинні використовувати різні правила фільтрації.

Коли пакет надходить до включеного брандмауера маршрутизатор фільтрації пакетів витягує заголовки з пакета і аналізує та перевіряє заголовки. Або перевіряються лише заголовки, пов’язані з протоколами TCP, IP, UDP. Потім правила фільтрації пакетів застосовуються послідовно до пакета, в тому порядку, в якому вони зберігаються в списку керування доступом брандмауера.

Правила застосовуються з урахуванням наступних принципів:

– якщо під час перегляду ACL знайдено правило, яке дозволяє коли посилка проходить, вона негайно відправляється за місцем призначення;

– якщо знайдено правило, що забороняє проходження пакета, воно негайно викинути;

– якщо при перегляді ACL виявляється, що немає правила, що дозволяють його проходження, пакет автоматично відкинуто.

Щоб створити правило фільтрації пакетів, вкажіть: action, виконується, коли критерії правила збігаються з параметрами пакета, протокол обробки пакетів і номер порту для отримання пакета. Неправильно порядок, в якому

написані правила, може призвести до повної блокування взаємоз'єднання або відкиньте правильні пакети і неправильна роздільна здатність.

2.3 Технології автентифікації

S / ключ. Система S / Key, визначена в RFC 1760, є схемою для генерації одноразового пароля на основі стандартів MD4 і MD5. Він призначений для боротьби з перехопленням паролів[8].

Протокол S / Key заснований на технології клієнт/сервер, де клієнтом зазвичай є персональний комп'ютер, а сервер — сервером аутентифікації. По-перше, і клієнт, і сервер повинні бути налаштовані на одну парольну фразу та обліковий запис ітерації. сервер відповідає надсиланням порядкового номера та випадкового числа «Зерно». Клієнт починає обмін S / Key, надсилаючи пакет ініціалізації на сервер, а потім клієнт генерує одноразовий пароль під час процесу, який складається з трьох кроків [8]:

– підготовчий етап;
– рівень генерації;
– вихідні функції.

На етапі підготовки клієнт вводить секретну парольну фразу, яка в незашифрованому вигляді підключається до «Korn», отриманого від сервера.

На етапі генерації клієнт потім багаторазово використовує хеш-функцію і отримує 64-бітове загальне значення. З кожним новим використанням кількість циклів хешування зменшується на один, створюючи унікальну послідовність згенерованих паролів. Заради сумісності клієнта і сервера вони повинні використовувати ту саму безпечну хеш-функцію.

Аутентифікація паролем токена. Апаратна автентифікація працює за однією з двох альтернативних схем: запит-відповідь або синхронізація часу.

У першому випадку користувач підключається до сервера аутентифікації, який у свою чергу вводиться персональний ідентифікаційний номер (PIN). Потім сервер передає випадкове число, яке користувач вводить у спеціальний

апаратний пристрій, де воно шифрується ключем користувача. Потім результат надсилається на сервер аутентифікації. Отримавши відповідь від користувача, сервер порівнює її зі своєю, яку отримав за допомогою ключа користувача, що зберігається в базі даних. Якщо обидва результати збігаються, доступ до мережі дозволено [8].

При використанні схеми синхронізації часу на апаратному забезпеченні користувача та на сервері працює секретний алгоритм, який генерує ідентичні паролі через певні синхронізовані інтервали та замінює старі паролі новими. Користувач може підключитися до сервера аутентифікації, який запитує доступ. Після цього користувач вводить свій PIN-код в апаратний пристрій і в результаті на екрані виводиться значення, яке є одноразовим паролем. Цей пароль надсилається на сервер [8].

Аутентифікація PPP. PPP — популярний інструмент інкапсуляції, який широко використовується в глобальних мережах. Він складається з трьох основних компонентів:

– метод інкапсуляції дейтаграм у послідовні канали;

– link control protocol (LCP), за допомогою якого встановлюється, налаштовується та тестується зв'язок;

– сімейство протоколів (NCP) для встановлення та налаштування різних протоколів мережевого рівня.

Щоб встановити пряме з'єднання між двома точками на каналі PPP, кожна з цих точок повинна спочатку відправити LCP-пакети, щоб налаштувати з'єднання на етапі його встановлення. Після встановлення з'єднання як приступила до роботи з протоколами мережевого рівня, протокол PPP дозволяє проводити аутентифікацію.

PPP PAP (Протокол аутентифікації пароля) не є надійним методом аутентифікації. Він лише аутентифікує оператора, що викликає, і паролі надсилаються на те, що вже вважається «безпечним». Таким чином, цей метод

не захищає від використання сторонніх паролів і повторних спроб вибрати пароль.

CHAP (Challenge Handshake Authentication Protocol) використовується для періодичної аутентифікації центрального комп’ютера або кінцевого користувача шляхом узгодження трьох параметрів. Аутентифікація відбувається під час спілкування, але може бути повторена пізніше.

CHAP забезпечує безпеку мережі, вимагаючи від операторів ділитися «текстовими секретами». Цей секрет ніколи не передається по каналу зв'язку. Після завершення кроку зв'язку аутентифікатор передає запит на пристрій, що викликає, який складається з ідентифікатора (ID), випадкового числа та назви центрального комп'ютера (для локального пристрою) або імені користувача (для віддаленого пристрою). пристрій). Машина, виділена жирним шрифтом, виконує обчислення з односторонньою хеш-функцією, вхід якої подається на аутентифікатор, випадкове число і загальний «текстовий секрет». Потім комп’ютер, що викликає, надсилає серверу відповідь, що складається з хеша та імені хост-комп’ютера або імені користувача віддаленого пристрою. Отримавши відповідь, аутентифікатор перевіряє ім’я, введене у відповіді, і виконує такі ж обчислення. Потім результат цих обчислень порівнюється зі значенням відповіді. Якщо ці значення збігаються, результат аутентифікації вважається позитивним, система видає повідомлення і LCP встановлює з’єднання [9].

Протокол TACACS + працює за технологією клієнт/сервер, за якою клієнтом зазвичай є NAS (сервер доступу до мережі), а сервер — «демон». Основним структурним компонентом протоколу TACACS + є розділення аутентифікації, авторизації та обліку (AAA - Authentication, Authorization, Accounting). Таким чином, ви можете обмінюватися повідомленнями аутентифікації будь-якої довжини та вмісту і таким чином використовувати будь-який механізм аутентифікації для клієнтів TACACS +, включаючи PPP PAP, PPP CHAP, апаратні карти та Kerberos. Аутентифікація не потрібна. Вважається варіантом, який налаштовується на сайті [9].

Трафік між клієнтом і сервером ідентифікуються загальним «секретом». Зазвичай він встановлюється вручну з обох сторін. TACACS + можливо налаштувати так, щоб весь трафік даних був зашифрований.

РАДІУС. Протокол RADIUS (RFC 2058, 2059) заснований на технології клієнт/сервер. Клієнт - це NAS, а сервер - "демон". Клієнт передає інформацію користувача на певний RADIUS-сервер, а потім діє відповідно до інструкцій, які він отримує. Сервери RADIUS приймають запити користувачів на підключення, аутентифікують користувачів, а потім надсилають всю інформацію про конфігурацію.

Реєстрація користувача зазвичай складається із запиту доступу, який надходить від NAS до сервера RADIUS, який шукає в базі даних вказане ім’я користувача. Якщо такого імені немає, сервер завантажить профіль за замовчуванням або надішле користувачеві негативну відповідь. У відповіді вказані пари атрибутів для цього сеансу.

Функції обліку RADIUS дозволяють надсилати дані про кількість ресурсів, використаних на початку та в кінці кожного сеансу.

Трафік між клієнтом і сервером RADIUS аутентифікуються за допомогою спільного «секрету», який ніколи не передається по мережевих каналах. Крім того, кожен користувач обмінюється тільки в зашифрованому вигляді, а це означає, що неможливо перехопити чужі паролі [9].

2.4 Технології цілісності і конфіденційності

SSL (Secure Socket Layer) — відкритий протокол, розроблений Netscape. Він визначає механізм безпеки даних між прикладним рівнем (HTTP, Telnet, NNTP, FTP, ...) і транспортним протоколом TCP/IP і підтримує шифрування даних, аутентифікацію сервера, цілісність повідомлень і (необов'язково) аутентифікацію клієнта в TCP / IP канал [10].

Основна мета протоколу - забезпечити безпеку та надійність зв'язку між двома підключеними додатками. SSL складається з двох рівнів: нижній знаходиться вище надійного транспортного протоколу TCP і називається протоколом запису SSL. Він використовується для вбудовування різних протоколів верхнього рівня, одним з яких є протокол рукостискання SSL, який дозволяє серверу і клієнту аутентифікувати один одного та узгоджувати алгоритм шифрування та криптографічні ключі.

SSL підтримує безпеку зв'язку, забезпечуючи наступні функції:

– безпека - після первинного підтвердження прийому та передачі зв'язку використовуються засоби шифрування та визначається секретний ключ. Для шифрування даних використовуються засоби симетричної криптографії (наприклад, DES, RC4 тощо).

– учасника сеансу зв'язку можна автентифікувати за допомогою відкритих ключів, тобто за допомогою асиметричної криптографії (наприклад, RSA, DSS тощо) [10].

– надійність – транспортні засоби перевіряють цілісність повідомлень за допомогою зашифрованого коду, розрахованого за допомогою захищених хеш-функцій (SHA, MD5 тощо).SSL прийнятий тільки в рамках HTTP. Хоча і інші протоколи довели свою здатність працювати з ним, використовують її вони не часто. [10]

SSH. Secure Shell (SSH) розроблено для захисту віддаленого доступу та інших мережевих послуг. Він підтримує безпечний віддалений вхід, безпечну передачу файлів і безпечний обмін повідомленнями TCP / IP і X11. SSH може автоматично шифрувати, аутентифікувати та стискати передані дані. Наразі він досить добре захищений від криптоаналізу та атак протоколів. За відсутності глобальної системи керування ключами та інфраструктури сертифікатів, SSH працює досить добре і може підтримувати існуючі інфраструктури (DNSSEC, X.509 тощо) у разі потреби [11].

Протокол SSH складається з трьох основних компонентів:

– протокол транспортного рівня, що забезпечує аутентифікацію сервера, конфіденційність, цілісність даних з відмінним захистом і стисненням реле [11];

– протокол аутентифікації користувача, який дозволяє серверу аутентифікувати клієнта;

– протокол з'єднання, мультиплексує зашифрований тунель і створює кілька логічних каналів.

Для шифрування використовуються алгоритми та схеми IDEA, 3DES, DES, RC4–128, Blowfish, AES. Обмін ключами здійснюється за допомогою RSA, а використані дані знищуються щогодини (ключі ніде не зберігаються) [11].

SOCKS v4 адресує незахищений інтерфейс брандмауерів із клієнтськими/серверними програмами на основі TCP, включаючи Telnet, FTP та популярні інформаційні протоколи, такі як HTTP, Wide Area Information Server (WAIS) і GOPHER. SOCKS v5, RFC 1928 включає UDP, розширює загальну структуру каркаса, дозволяє використовувати потужні узагальнені схеми аутентифікації та розширює систему адресації, щоб включати ім’я домену та IP-адресу v6. [11].

Функція SOCKS полягає в заміні стандартних мережевих системних викликів у програмі на їх спеціальні версії, які спілкуються з проксі-сервером SOCKS (він налаштовується користувачем у програмі або файлі конфігурації системи), підключається до відомого порту (зазвичай порт 1080). / TCP). Після підключення до сервера SOCKS програма надсилає серверу ім'я комп'ютера та номер порту, до якого користувач хоче підключитися. Сервер SOCKS фактично спілкується з віддаленим комп’ютером, а потім прозоро передає дані між програмою та віддаленим комп’ютером. Користувач поняття не має, що канал зв'язку має сервер SOCKS.

Складність використання SOCKS полягає в тому, що комусь доводиться працювати над заміною мережевих системних викликів версіями SOCKS (цей

процес зазвичай називають програмою «SOCKS-іфікація»). На щастя, більшість популярних мережевих програм (Telnet, FTP, Finger, Whois) вже підтримують SOCKS, і багато постачальників пропонують підтримку SOCKS у своїх комерційних програмах [11].

IPSec. Цей протокол використовується для захисту даних та аутентифікації на рівні IP. Поточні стандарти IPSec містять базові специфікації, незалежні від алгоритмів, RFC 2401 - 2412.

IPSec покладається на використання двох протоколів для взаємодії: ESP (Encrypting Security Payload), який відповідає за шифрування, і IKE (Internet Key Exchange), який використовується для узгодження методів і ключів [12].

Існує два режими роботи IPSec: транспортний і тунельний.

У транспортному режимі шифрується лише поле пакетних даних IP, а заголовок залишається неушкодженим. Якщо хакер прослухає сесію, він отримає лише адреси сторін, а інформація залишиться закритою [12].

У тунельному режимі пакет повністю шифрується і додається новий заголовок. Цю схему взаємодії зручно використовувати для зв’язку між двома філіями організації за допомогою технології VPN. Перехоплені (наприклад, на магістралі провайдера) повідомлення навіть не дозволяють зловмиснику розкрити внутрішню структуру приватної мережі [12].

X.509. X.509 визначає формати даних і процедури для видачі відкритих ключів з використанням сертифікатів із цифровим підписом, які надаються органами ЦС (центром сертифікації) [12].

Кожен сертифікат складається з трьох основних полів: текст сертифіката, алгоритм підпису та сам підпис.Текст сертифіката містить номер версії, серійний номер, назви емітента та суб’єкта, відкритий ключ суб’єкта, термін дії (дата і час початку і закінчення дії сертифіката). Іноді цей текст містить додаткову необов’язкову інформацію, яка розміщується в унікальних полях, які призначають додаткові атрибути користувачам або спільним ключам. Алгоритм підпису — це алгоритм, який центр сертифікації використовує для підписання

сертифіката. Підпис створюється шляхом пропуску тексту сертифіката за допомогою односторонньої хеш-функції. Значення, отримане на виході, шифрується за допомогою приватного ключа CA. Результатом такого шифрування є цифровий підпис [13].

CRL — це список відкликаних сертифікатів із міткою часу. Він підписаний ЦС і вільно поширюється через загальнодоступні списки відкликаних сертифікатів. Кожен відкликаний сертифікат ідентифікується в списку CRL за його серійним номером. Коли системі потрібно використовувати сертифікат (наприклад, для перевірки цифрового підпису віддаленого користувача), система не тільки перевіряє підпис і дату закінчення терміну дії сертифіката, але також перевіряє останні доступні CRL, щоб перевірити, чи був сертифікат відкликаний [13].

2.5 Технології віддаленого доступу VPN

Протокол пересилання рівня 2 (L2F) був розроблений Cisco Systems. Це дозволяє тунелювати протоколи канального рівня з використанням протоколів вищого рівня, таких як, наприклад, B. IP. За допомогою таких тунелів можна відокремити розташування сервера RAS, до якого користувач підключається за допомогою локальних комутованих з’єднань, від точок, де безпосередньо обробляється протокол RAS (SLIP, PPP) і користувач отримує доступ мережі [14].

Тунелі, побудовані на L2F, дозволяють використовувати програми, які потребують віддаленого доступу з приватними адресами IP, IPX і AppleTalk через SLIP/PPP через існуючу інфраструктуру Інтернету [14].

Протокол тунелювання "точка-точка". Протокол тунелювання «точка-точка» (PPTP) був розроблений Microsoft. Він нічого не змінює в ППП, але надає для нього новий транспортний засіб. Цей протокол визначає архітектуру клієнт/сервер, яка була розроблена для спільного використання функцій,

доступних у поточних NAS (серверах доступу до мережі), і для підтримки віртуальних приватних мереж (VPN). Мережевий сервер PPTP (PNS) повинен працювати в операційній системі загального призначення, а клієнт, відомий як PPTP Access Concentrator (PAC), працює на платформі RAS [14].

PPTP визначає протокол керування викликами, який дозволяє серверу контролювати віддалений доступ через телефонні мережі загального користування (PSTN) або цифрові канали ISDN або форматувати вихідні комутовані з'єднання. PPTP використовує механізм Generic Routing Encapsulation (GRE) для передачі пакетів PPP, контролюючи потоки даних і перевантаження мережі. Безпека даних у PPTP може бути гарантована за допомогою протоколу IPSec [14].

L2TP. Протоколи L2F і PPTP мають схожі функції. Cisco і Microsoft домовилися (в рамках IETF) розробити єдиний стандартний протокол під назвою Layer 2 Tunneling Protocol (L2TP). Обидві компанії продовжать підтримку власних рішень віртуальної приватної мережі (L2F і PPTP) і перехід від цих рішень до L2TP [14].

3 ВИЯВЛЕННЯ НОВИХ ВРАЗЛИВОСТЕЙ У SONARQUBE ТА GRAFANA ЗА ДОПОМОГОЮ SIEM

3.1 SIEM системи

SIEM – об'єднання двох визначень, що означають область застосування програмне забезпечення: SEM - управління подіями безпеки та SIM - Управління інформаційною безпекою. Системи SIEM забезпечують аналіз вихідних подій безпеки з програм і мережевих пристроїв у режимі реального часу. SIEM складається з з програм, пристроїв, служб, а також для реєстрація даних.

Такі системи допомопомогають вирішити наступні завдання.

1. Консолідація та зберігання різних журналів подій джерела - мережеві пристрої, журнали операційної системи, програми та системи інформаційної безпеки. Після перегляду будь-якого стандарту інформаційної безпеки ми побачимо технічні вимоги до нього збір та аналіз подій. Вони потрібні не тільки для відповідати вимогам стандарту, оскільки бувають ситуації, коли інцидент було помічено пізно, а події видалено або записано на тривалий час події з якихось причин недоступні і причини того, що сталося, виявити майже неможливо

2. Надати інструменти для аналізу та аналізу подій інциденти. Створює читабельну відповідь. У тому числі безпосередньо з необхідною фільтрацією. Наприклад, щоденний звіт про інциденти, перевірка стану здоров’я тощо.

3. Співвідношення та трактування правил. Найпростіший приклад «Помилка підключення»: один випадок нічого не означає, а три або більше події з обліковим записом вже можуть вказувати спроби відбору. У найпростішому випадку представлені правила SIEM у форматі RBR (Rule Based Reasoning) і містять набір умов тригери, лічильники, сценарій дії.

4. Автоматичне сповіщення та управління інцидентами. Головний завданням таких систем є не простий збір подій, а й автоматизація процес виявлення інцидентів зі збором журналів, і своєчасно повідомляти про подію.

Системи збору та кореляції подій є універсальними завдяки своїм логічним діям, але щоб отримати від них очікуваний результат, необхідні корисні джерела та правила для кореляції подій (рис. 3.1). Можна ввести будь-яку подію (наприклад, із системи DLP). систем і використовується

Джерела вибираються з урахуванням таких факторів:

– критичність системи та інформації;

– достовірність та інформативність джерела події;

– Покриття каналів передачі інформації (враховуючи не тільки зовнішній контур, а й внутрішній).;

– Вирішувати низку завдань, пов’язаних із IT та інформаційною безпекою.

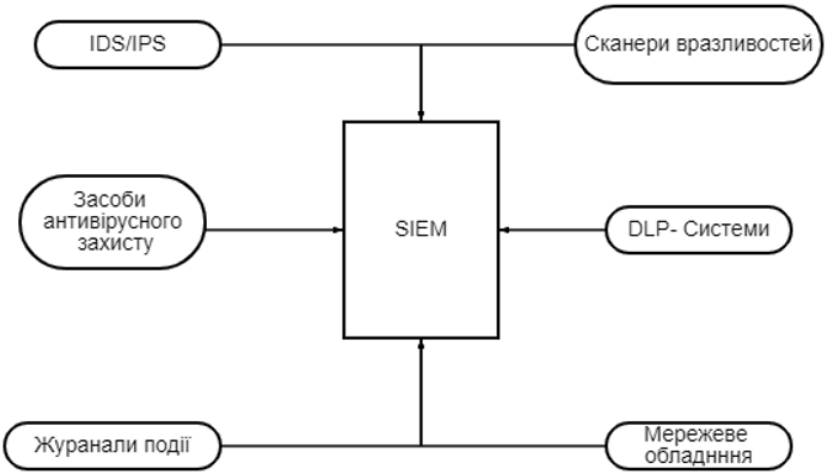

Рисунок 3.1 – Джерела подій SIEM-систем

Найчастіше такі системи складаються з кількох компонентів:

– агенти, встановлені на контрольованій системі і відправити дані на сервер;

– корелятори на агентах є модулями для розуміння журнал конкретних подій;

– кореляторні сервери, попередньо накопичені події з кількох перевірених джерел;

– сервер кореляторів, відповідальний за збір інформації від кореляторів і агенти та обробка за заданими правилами та алгоритмами;

– сервер бази даних і зберігання, відповідальний за зберігання журналів події.

Дані про події збираються з джерел за допомогою агентів, або дистанційно. У разі віддаленого збору подій стягується плата до мережі та джерела подій, оскільки деякі системи не дозволяють передавати лише події, які ще не були передані, і передати весь журнал подій, що складається з великого числа інформації.

Крім того, події повинні збиратися не тільки в репозиторії для аналізу за фактом інциденту, але й оброблятися. Інший система не виправдовує витрати. Безумовно, інструментарій SIEM скоротить час на розслідування інциденту, але завдання системи є вчасно, а також швидко виявляти та запобігати загрозам реагувати на них. Ось чому повинні дотримуватися правил кореляції встановлюється індивідуально, відповідно до особливостей компанії. Ці правила діють недовго і вимагають частого оновлення. Забагато найбільше у випадку систем виявлення вторгнення, інакше в часі прописати правила, які дозволяють виявити загрозу - вона неодмінно буде буде реалізовано. Перевага системи збору подій і кореляції захист інформації від систем виявлення вторгнення в правила - можливість вказати загальний опис симптоми і використання статистичних даних, накопичених для спостереження відхилення від нормального стану інформаційних систем.

SIEM здатний корелювати:

– загроза, описана правилами;

– загроза на основі загальної моделі;

– аномалія у разі відключення від бази накопиченої статистики (на основі);

– відступ від принципу «все, що заборонено, заборонено»;

– причинно-наслідковий зв'язок, якщо відокремлено алгоритми.

Останні три алгоритми використовуються в Україні дуже рідко. З такими методами може працювати невелика кількість систем кореляція. Можливість роботи з цими алгоритмами зростає витрати на обслуговування системи через потребу в кваліфікований фахівець, який встановить і підтримувати систему актуальною та ефективною. Часто кількість помилкових спрацьовувань напочатку операції система велика, тому в більшості випадків компанії задоволені вимкнути ці механізми виявлення.

Звідси випливає, що фактично використовуються лише два найпростіших алгоритм виявлення з попередньо визначеним описом загрози.

Їхня робота вимагає постійного оновлення загроз, як і для IDS. В результаті відбувається дублювання загроз в IDS і SIEM, тільки в цьому випадку правила кореляції оновлюються набагато рідше, а не правила IDS. Багато підприємств не можуть собі дозволити у штаті кваліфікованого аналітика SIEM та правила кореляції, тому нерідкі випадки, коли правила частково оновлюються продуктів просто не вистачає. З цього випливає, що у справі як тільки правила кореляції будуть налаштовані, інцидент буде виявлено, тільки якщо цього вимагає інший засіб.

3.2 Принципи обробки SIEM системи

Системи SIEM автоматично комбінують та координують події Безпека інформації, отриманої від різних пристроїв захисту, що дозволяє аналітики зосереджуються на більш складних, критичних завданнях. Наразі не існує універсальної системи виявлення та запобігання вторгненню. Оскільки всі рішення безпеки мають їх слабкості та переваги, а всі ресурси захищені і інформаційні системи надзвичайно різноманітні. Системи виявлення вторгнень

можна комбінувати і таким чином поліпшити роботу системи безпеки в цілому, але за рахунок їх різноманітність можуть дати системи виявлення вихідна інформація з точки зору рівня тривожності, оскільки вона пов'язана з рівнем конфіденційності захищеної інформації.

Вторгнення відбувається, коли зловмисник намагається завдати удару в захищеній системі або використовувати її неправильно. Термін «Зловживання» можна трактувати по-різному відноситься до багатьох дій, починаючи з розкриття конфіденційної інформації і закінчуючи звичайною відправкою спам. Наприклад, більшість подій тривоги, які генеруються системи контролю доступу до ресурсів на серверах і комп'ютерах персонал безпосередньо не відображає напади. Вони описують дії користувача, який працює із захищеними ресурсами, тому, аналізуючи ситуацію, ми повинні враховувати контекст, в які тривожні події відбулися. Розглянемо деякі з них:

– подія «введено неправильний пароль» зустрічається дуже часто у всіх тому слід ігнорувати, але якщо шістнадцять неодноразово відбувалося в неробочий час компанії, це має бути створено попередження високого рівня;

– якщо поведінка дивна, користувач перебуває на тому самому сервері, то це може і, швидше за все, помилкова аномалія і може бути ігнорується. Однак, якщо це відбувається на кількох сервери, то хтось досліджує мережу явно (наприклад, переглядаючи порти);

– на деяких комп’ютерних системах подія класу «збій вхід в систему "може відбуватися кілька разів на день, поки в інших середовищах таких подій взагалі не повинно бути.

Вище були описані деякі події, які є найбільшими невелика частина даних виявлення вторгнення. події, переконайтеся, що ви зареєстровані. Згодом ці дані будуть брати участь у трьох кроках у боротьбі з вторгненнями:

– виявлення;

– реакція;

– запобігання.

Система кореляції отримує інформацію на всіх цих етапах і поєднує його за попередньо заданими алгоритмами. Це робить процес виявлення є керованим і надає інформацію, необхідну для майбутня профілактика та відповідне реагування. Витрати Зауважимо, що кореляція подій у великій компанії є виснажливе завдання обробки великих обсягів даних. Для таких випадків, на допомогу створюються автоматизовані системи об'єднати велику кількість інформації, позбутися зайвого даних, знайти необхідні події та діяти на основі зібраних даних з обладнання. Кожне з цих завдань може бути виконано за допомогою системи збору і співвідношення подій інформаційної безпеки.

На основі кореляційних даних, отриманих у момент виникнення подій, у доступі до атакованого пристрою може бути відмовлено, таким чином, збитки, завдані вторгненням, будуть зменшені. Без централізоване управління системою та механізми кореляції, визначити тип нападу, оцінити придатність практично неможливо системи захисту і діють в режимі реального часу. Більше ефективною, система буде в тому випадку, якщо системи виявлення вторгнення, брандмауери, брандмауери та системи Безпека додатків працюватиме разом і співпрацюватиме дії знизять ризик виникнення, поведінки і здійснення загроз. Таке рішення виконує такі функції:

– отримує інформацію з одного або кількох джерел;

– розглядати повідомлення відповідно до їх характеристик;

– опрацювати повідомлення за правилами їх співвіднесення;

– зберігає повідомлення в реляційній базі даних.

Оскільки технологія тільки розвивається, ще немає чітка теорія цих систем, але стандартні методи вже розроблені кореляції, які можна застосувати.

З огляду на цю роботу можна зробити висновок, що кореляція являє собою процес порівняння, інтерпретації, поєднання і вирівнювання дані різних компонентів захисту (агентів), вироблених с метой визначення спроб нападу на них, або несанкціонований доступ.

Оскільки це новий шлях у сфері інформаційної безпеки, повного набору методів ще не існує. Наразі існує два типи кореляції:

– мікрокореляція. Стосовно технологій кореляції подій, які зосереджені на порівнянні даних в одному потоці подій;

– макрокореляція. Порівняйте дані в потоці подій з даними, зібраними з інших джерел.

Якщо мікрокореляцію можна назвати відправною точкою в реалізація механізмів кореляції подій, то макрокореляція дає ми маємо можливість об'єднання кількох потоків, що дозволяє збільшити швидкість і точність виявлення атак. Вважається, що необхідно для краще управління інформаційною безпекою використовувати обидва підходи.

Вище ми розглянули основні методи кореляції. Але перш ніж почати будувати систему, ми повинні зробити більше етапів попередньої обробки даних, а саме:

– транспортування даних. Ми повинні отримати вихідні дані з унікальні засоби забезпечення інформаційної безпеки і відправити їх до зведеної бази даних кореляційної системи. Консолідація даних – процес об’єднання облікових даних отримав з кількох джерел визначену основу, від який описуватиме стан мережі. На цьому рівні забезпечується захист і цілісність вихідних даних кореляції – спосіб їх перевірки за допомогою електронного підпису і шифрування;

– стандартизація даних. Майже всі програми ведуть облік попередження, помилки та збої власних служб вреєстраційні файли. Брандмауери та VPN-шлюзи можуть відстежити всі сумнівні з'єднання при вході в мережу і вийти. Комутатори та маршрутизатори зберігають журнали стану мережі в управлінських інформаційних базах. Часто системи надсилають важливі попередження (наприклад, пастки SNMP) на панелі керування консоль управління. Тому дані переміщено до консолідованої бази, зводяться до певного уніфікованого формату. Все це має дбати про збереження охорони «сирого» дані,

наприклад, у разі судового розгляду, тому що змінена інформація більше не може використовуватися як доказ. У цей момент загальний набір даних «стискається», коли зберегти їх цілісність і повноту;

– скорочення даних. Під час впровадження системи виявлення вторгнення, великі організації стикаються з величезним обсягом дані, які можуть бути переважними для професіоналів.

Певним чином наприклад, великий універсальний сервер, який працює весь час, здатний генерувати до одного терабайта журналів даних на годину. У цьому представляють ситуації отримання та організації вхідних даних важлива проблема, що вимагає спеціального дослідження робота в області систем виявлення вторгнень. А оскільки це все терабайти даних важливі для наступного аналітичної обробки, вони потім потрібні на деякий час зберегти. Зменшення набору даних передбачає використання широкий спектр методів і операцій, спрямованих на кінцеву прискорення програми кореляції. Зниження може бути виконується шляхом стиснення даних, стирання повторюваних наборів, відфільтрувати деякі несуттєві речі інформації, комбінування схожих подій єдино і так далі.

Вивчаються події з різних джерел дублювання інформації та зайві дані видаляються. Далі спеціальними правилами обробляються реєстраційні, інформаційні і тривожні повідомлення. Творець системи на цьому етапі приймає рішення що слід зберегти, а що усунути. Так за все організацію, можливо, створити власну дуже тривіальні правила обробки подій - наприклад, фільтрація подій здійснюється відповідно до цих рівнів ризику (і в цьому замовлення), які приймаються компанією. Скільки оригінальних "необроблені" дані повинні бути збережені, а тривалість залежить від політики захисту. Що і як накопичити на майбутнє лікування - це одна з головних проблем організації, які відповідають завданням ефективного управління події. Цей останній крок, серед іншого, наступний використовувати обережно, щоб не знищити важливий елемент переконлива інформація.

Після того, як дані зібрані в одній точці, нормалізуються і знижені системи управління інформаційною безпекою можна почати процес кореляції.

Кореляція дуже корисна для виявлення порушень безпеки, оскільки ці інциденти є серією подій, що відбуваються в різних точках «дотику» мережі. Цей процес характеризується відносинами багато до одного (тобто майже всі події від великої кількості датчиків вказують на атаку). В порівняння з мережевим керуванням, яким зазвичай користується відносини виключення подій (необхідне - непотрібне) або індивідуальні відносини, управління інформаційною безпекою набагато складніше. Проникнення зазвичай залишає сліди в різних точки мережі та в іншому часовому порядку. Знайди все сліди, фахівці з інформаційної безпеки, зможе знайти і з найвищим ступенем надійності запобігти напад.

Тому, дотримуючись людської логіки, у справі слід поступити так само створення системи SEM. Після отримання всіх даних і обробляються в єдиній базі даних, необхідно визначити, як і в якій послідовності, ці події постають таким чином, що у своїй сукупності імітувати одну подію вторгнення. Дещо дослідницькі компанії використовують термін «рядок ефемерні події. «Як тільки такий ланцюг побудують, фахівець може перейти до аналізу самих подій і до нарізки включаючи моделі.

3.3 Огляд існуючих SIEM систем

У процесі своєї роботи кожен пристрій, від персональний комп'ютер із складними системами штучного інтелекту, записує всі події, які відбуваються в його системі в журналах реєстру. Записані в цих журналах, адміністратор може оцінити діяльність системи та точно розповісти, які операції відбувалися в системі в будь-який момент часу. Аналіз журнальних записів є одним з основних методів дослідження на сьогоднішній день. потенційно небезпечні дії в системі. Але через складність інфраструктури і різноманітність пристроїв, кількість

журналів подій може досягати кількох десятків і проаналізувати їх окремо один від одного практично неможливо. Лише для створено рішення проблеми централізованого збору та аналізу всіх подій перші системи, пізніше названі SIEM.

Концепція SIEM (Security Information and Event Management) сьогодні досить розпливчаста, ви можете уявити, що це процес, який об’єднує мережеві дії в єдиний адресний запис. Сам термін був введений Gartner в 2005 році, але сама концепція і все, що з ним пов’язано, з тих пір сильно змінилися. Спочатку абревіатура представляла собою комбінацію двох термінів, які позначали сферу застосування програмного забезпечення: SIM (Security Information Management) - управління інформаційною безпекою і SEM (Security Event Management) - управління подіями безпеки. За словами Gartner, система SIEM повинна збирати, аналізувати та представляти інформацію з мережевих пристроїв і пристроїв безпеки. Він також повинен включати програми керування ідентифікацією та доступом, інструменти керування вразливими місцями, а також бази даних і програми. Для наочності виділено деякі функції, які зазвичай надаються системами SIEM:

– можливість надсилати сповіщення на основі попередньо визначених налаштувань;

– звіти та журналювання для спрощення тестування;

– можливість перегляду даних на різних рівнях деталізації.

Як правило, розмір пам'яті залежить від кількості подій, що обробляються в мережі компанії. До лідерів на світовому ринку SIEM можна віднести наступні:

– HP ArcSight;

– IBM QRadar SIEM;

– Tibco Loglogic;

– McAfee NitroSecurity;

– RSA Envision Splunk;

– LogRhythm.

На думку деяких експертів, SIEM – це вдосконалена система виявлення шкідливої активності та різних системних аномалій. Операції SIEM дають вам більш повну картину мережевої активності та подій безпеки. Коли традиційним детекторам не вдається ідентифікувати атаку окремо, ретельний аналіз і співвіднесення інформації з різних джерел може виявити її. Тому багато компаній вважають використання системи SIEM додатковим і дуже важливим елементом захисту від цілеспрямованих атак.

Раніше ми розглядали популярні варіанти використання SIEM:

– відстеження автентифікації та виявлення вразливостей облікового запису користувача та адміністратора;

– відстеження випадків зараження. Виявлення зловмисного програмного забезпечення за допомогою вихідного брандмауера та протоколів веб-проксі, а також протоколів внутрішнього підключення та мережевого потоку;

– відстежуйте підозрілий вихідний та мережевий трафік за допомогою журналів брандмауера, журналів веб-проксі та NetFlow. Виявлення крадіжки даних та інших підозрілих зовнішніх з'єднань;

– відстеження системних змін та інших адміністративних заходів у внутрішніх системах та дотримання допустимих рекомендацій;

– відстеження атак на веб-програми та їх наслідки за допомогою журналів веб-сервера, брандмауера веб-програм (WAF) та журналів програм. Виявлення спроб компромісу для веб-додатків шляхом аналізу різних звітів.

З цієї причини рішення SIEM - повинно бути в центрі сучасної системи інформаційної безпеки. SIEM допомагає компаніям виявляти та запобігати кібератакам на ранній стадії, аналізуючи дані з IT-інфраструктури компанії в режимі реального часу, щоб визначити потенційні загрози безпеці.

HP є лідером на українському ринку продуктів SIEM зі своїм рішенням HP ArcSight. Система дозволяє підключати широкий спектр додаткових модулів від HP та сторонніх постачальників (рис. 3.2).

Рисунок 3.2 – Магічний квадрат Гартнера для SIEM-систем.

Варто відзначити, що HP пропонує повний спектр рішень для інформаційної безпеки. Тому рішення HP Fortify спрямоване на покращення та зменшення кількості вразливостей у корпоративному програмному забезпеченні. HP ArcSight відповідає за пошук і запобігання відомим і невідомим загрозам. HP TippingPoint активно захищає від відомих атак і атак нульового дня. HP Atalla захищає дані, криптографічні ключі та безпечні платіжні транзакції.

Однак саме рішення HP ArcSight можна назвати центром системи інформаційної безпеки. Як зазначили доповідачі, це рішення може бути як складним, так і простим залежно від потреб замовника. Продукт пропонує широкий спектр функцій для збору, консолідації та співвіднесення подій; пропонує розширені функції кореляції; Відповіді на “Що? Куди? Якщо?“, Готові правила, звіти та графіки [15].

IT-компанія SVIT пропонує послуги з впровадження, включаючи базові поради та навчання щодо використання системи, а також пост-проектну підтримку та рекомендації щодо подальшого розвитку та вдосконалення.

HP ArcSight Express – цей інструмент SIEM надає інформацію та інструменти, необхідні для визначення та визначення пріоритетів поточних і потенційних загроз для оптимізації реагування та підвищення безпеки системи.

HP ArcSight Express 6.9 – це радикально новий продукт. Ліцензується лише за кількістю подій, без обмежень щодо користувачів чи джерел. Веб-консоль – ArcSight Command Center – шукає події (наприклад, реєстратори та ESM) через Інтернет; Повнотекстовий пошук. Продукт заснований на сервері HP DL380 Gen9 (2x12-ядерний процесор, 196 ГБ, 8x600 ГБ).

ArcSight ESM пропонує розширені можливості кореляції, готові правила, звіти та графіки, безпечне та ефективне зберігання даних та відповіді в реальному часі. Стандартні звіти містять такі назви: Моніторинг конфігурації, Моніторинг мережі, Робочий процес, Моніторинг NetFlow, Моніторинг вторгнень, Моніторинг Cisco та Моніторинг Microsoft Windows (рис. 3.3).

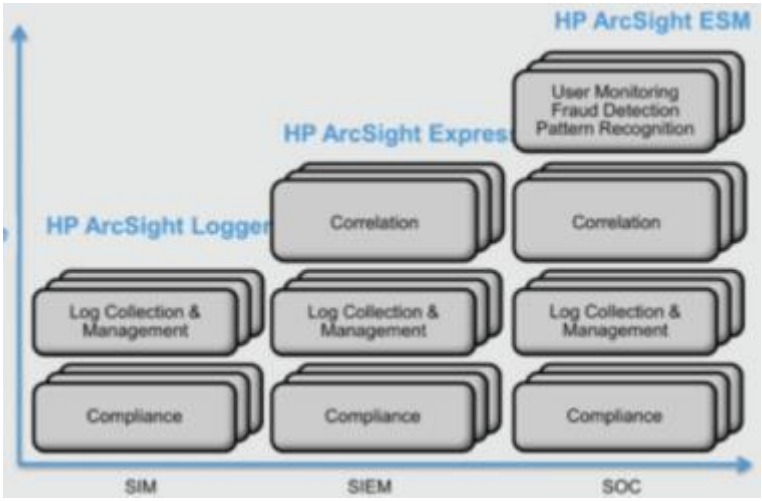

Рисунок 3.3 – Можливості розширення HP ArcSight .

3.4 Виявлення вразловостей у SonarQube та Grafana

SonarQube — це платформа з відкритим вихідним кодом, розроблена SonarSource для постійної оцінки якості коду за допомогою статичного аналізу.

Іншими словами, він не запускає код, він просто переглядає його. Не дивно, що SonarQube має досить вражаючий список клієнтів і репутацію одного з найбільш затребуваних інструментів статичного аналізу коду.

Після завершення аналізу коду, який буде обговорено пізніше, SonarQube створює звіт, який можна переглянути в графічному інтерфейсі користувача через браузер. Усі проблеми, з якими стикаються, — це «онлайн-квитки», що дозволяють писати до них коментарі, делегувати їх іншим користувачам, відкривати або закривати їх тощо (рис. 3.4).

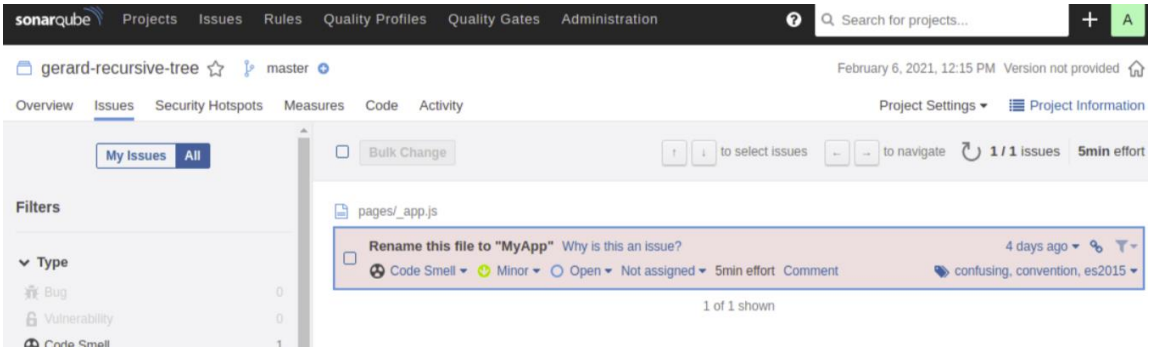

Рисунок 3.4 – Приклад SonarQube .

Детальний опис проблеми одразу супроводжується відповідним кодом (рис. 3.5).

Рисунок 3.5 – Приклад опису проблеми SonarQube.

Можливо подумати, що звичайні інструменти, такі як ESLint, роблять те саме безпосередньо під час написання коду, але я це не так. SonarQube забезпечує набагато вищу якість з широкого кола тем, таких як дивний код, помилки та вразливості безпеки.

SonarQube надає систематичний звіт про якість коду, безпеку та загальний стан шлюзу якості, тобто логічне значення, яке вказує на те, що програма готова до відправки у виробництво. Якщо ви додасте сканування сонара до конвеєра, звіт оновлюватиметься з кожним запитом перевірки або вилучення. Крім того, він підтримує керування версіями, кожне з яких виконує певну фіксацію або злиття гілок у проекта.

Це не просто звіт, а складний структурований «живий» набір даних, який постійно контролює проект і інформує його власників про поточний стан якості. Таким чином, це дозволяє іншим учасникам проекту працювати разом над цим станом. Проблеми можна обговорювати та делегувати, що дуже сприяє співпраці.

Саме в можливості співпраці є найбільш істотною перевагою SonarQube перед такими інструментами, як ESLint, завдяки якому «розробник вирішує проблему самостійно».

Спосіб авторизації в SonarQube досить стандартний. Можна створити необхідну кількість користувачів і груп користувачів. Потім користувачів можна приєднати (або ні) до (кількох) груп. Потім групам та/або користувачам надаються (кілька) дозволи. Дозволи надають доступ до проектів, служб і функцій.

За замовчуванням SonarQube примушує автентифікацію користувача. Але є можливість вимкнути примусову автентифікацію користувачів і дозволити анонімним користувачам переглядати проекти та виконувати аналіз. Для цього потрібно увійти як системний адміністратор, далі у Адміністрування > Конфігурація > Загальні параметри > Безпека та вимкніть властивість Примусова автентифікація користувача (рис. 3.6).

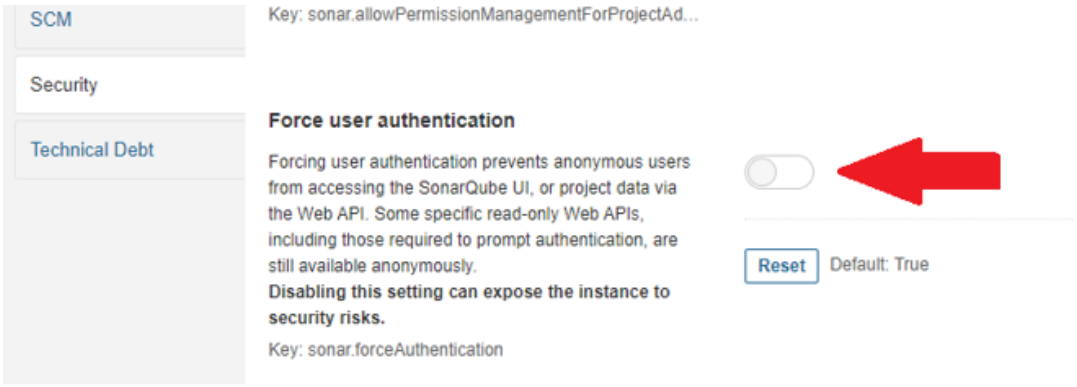

Рисунок 3.6 – Приклад вимкнення властивість аутентифікації

Вимкнення примусової автентифікації користувача може піддати ваш екземпляр SonarQube ризикам безпеки. Наполегливо рекомендуємо примусово автентифікувати користувачів у робочих екземплярах або ретельно налаштувати безпеку (дозволи користувача, видимість проекту тощо) у вашому екземплярі.

Далі за допомогою команди “curl” ми можемо побачити можливість дивитися стартову сторінку без введення секретів (рис. 3.7).

Рисунок 3.7 – Виконання команди “curl” на цільовий сервер

Для усунення вразливості потрібно увійти як системний адміністратор, далі у Адміністрування > Конфігурація > Загальні параметри > Безпека та увімкнути властивість Примусова автентифікація користувача

Grafana написана мовою програмування Go (створений Google) і Node.js LTS разом із сильним інтерфейсом прикладного програмування (API). Ця програма, яка стає все більш популярним, з ентузіазмом спільноти, що складається з більш ніж 600 добре інтегрованих учасників (є 7 провідних розробників, відповідальний Torkel і 5 співробітників, зайнятих неповний

робочий день, щоб мати можливість координувати такі компанії людей). Звичайно, його вихідний код був опублікований на GitHub.

Панель управління добре оснащена для розуміння складних даних, таких як графіки, теплові карти, гістограми та географічні карти, і вона постійно оновлюється. Інструмент надає безліч рішень візуалізації для розуміння даних відповідно до бізнес-потреб конкретного проекту. Ось ключові особливості Grafana, які вам потрібно знати:

– створення шаблонів панелі приладів. Одна з найважливіших функцій Grafana, що створює шаблони інформаційних панелей, допомагає вам створювати інформаційні панелі, які можна повторно використовувати для різних цілей і спільно використовувати в командах вашої організації;

– підготовка. Хоча створити єдину панель моніторингу просто, клацнувши, перетягнувши і відпустивши її, користувачі, які потребують багато панелей моніторингу, захочуть використовувати сценарій для автоматизації процесу. Grafana дозволяє створювати сценарії для чого завгодно та отримувати контроль над великою кількістю інформаційних панелей;

– анотації. У Grafana ця функція відображається як маркер графіка і корисна для зіставлення даних у випадку, якщо щось піде не так. Ви можете створювати інструкції вручну (клацніть графік і введіть текст, утримуючи клавішу Control) або отримати дані з будь-якого джерела даних;

– режим плейлисту. Якщо ви бажаєте відображати свої інформаційні панелі Grafana на телевізійному моніторі, ви можете використовувати функцію списку відтворення, щоб вибрати, які інформаційні панелі потрібно переглядати, і змусити їх циклічно переміщатися по екрану. У режимі тільки для перегляда режим кіоску приховує всі елементи інтерфейсу користувача, які вам не потрібні;

– користувальницькі плагіни. Ви можете використовувати плагіни для розширення Grafana та інтеграції його з іншим програмним забезпеченням, візуалізаціями і т. д. Все, що створює позначку часу та значення, можна візуалізувати в Grafana за допомогою всього кількох рядків коду;

– оповіщення та пастки для попереджень. Якщо відбувається очікуваний сценарій, попередження активуються як розтяжки. Про ці події можна повідомити команду моніторингу через Slack або через інший канал зв'язку;

– дозволи та команди. Коли в компанії є одна Grafana і кілька команд, часто хочуть розділити речі, але при цьому використовувати інформаційні панелі. Якщо ви використовуєте Grafana Enterprise, ви можете створити команду користувачів, а потім встановити дозволи для папок, інформаційних панелей та аж до рівня джерела даних;

– джерела даних SQL. Вбудована підтримка SQL у Grafana дозволяє вам перетворювати все, що є в базі даних SQL, на дані метрик, які ви можете графічно відображати. Джерела даних SQL використовуються досвідченими користувачами для виконання безлічі цікавих речей, наприклад для створення бізнес-панелей;

– аутентифікація. Grafana підтримує різні стилі автентифікації, включаючи LDAP та OAuth, та дозволяє відображати користувачів в організації.

Grafana, звичайно, має вбудовану систему аутентифікації користувачів з автентифікацією паролем, увімкненою за замовчуванням. Але можливо вимкнути автентифікацію, увімкнувши анонімний доступ. Також можете приховати форму входу та дозволити вхід лише через постачальника аутентифікації (перерахований вище). Також є варіанти дозволу самостійної реєстрації (рис. 3.8).

```
[auth]
# Login cookie name
login_cookie_name = grafana_session
# The lifetime (days) an authenticated user can be inactive before being required to login at next visit. Default is 7 days.
login_maximum_inactive_lifetime_duration = 7d
# The maximum lifetime (days) an authenticated user can be logged in since login time before being required to login. Default is 30 days.
login_maximum_lifetime_duration = 30d
# How often should auth tokens be rotated for authenticated users when being active. The default is each 10 minutes.
```

```
token_rotation_interval_minutes = 10
# The maximum lifetime (seconds) an api key can be used. If it is set all the api keys should have limited lifetime that is lower than this value.
api_key_max_seconds_to_live = -1
```

Рисунок 3.8 – Приклад налаштувань Grafana

Можливо зробити Grafana доступною без входу в систему, увімкнувши анонімний доступ у файлі конфігурації(рис. 3.9).

```
[auth.anonymous]
enabled = true
# Organization name that should be used for unauthenticated users
org_name = Org.
# Role for unauthenticated users, other valid values are `Editor` and `Admin`
org_role = Viewer
# Hide the Grafana version text from the footer and help tooltip for unauthenticated users (default: false)
hide_version = true
```

Рисунок 3.9 – Приклад налаштувань анонімного доступу до Grafana

Далі за допомогою команди “curl” ми можемо побачити можливість дивитися стартову сторінку без введення секретів (рис. 3.10).

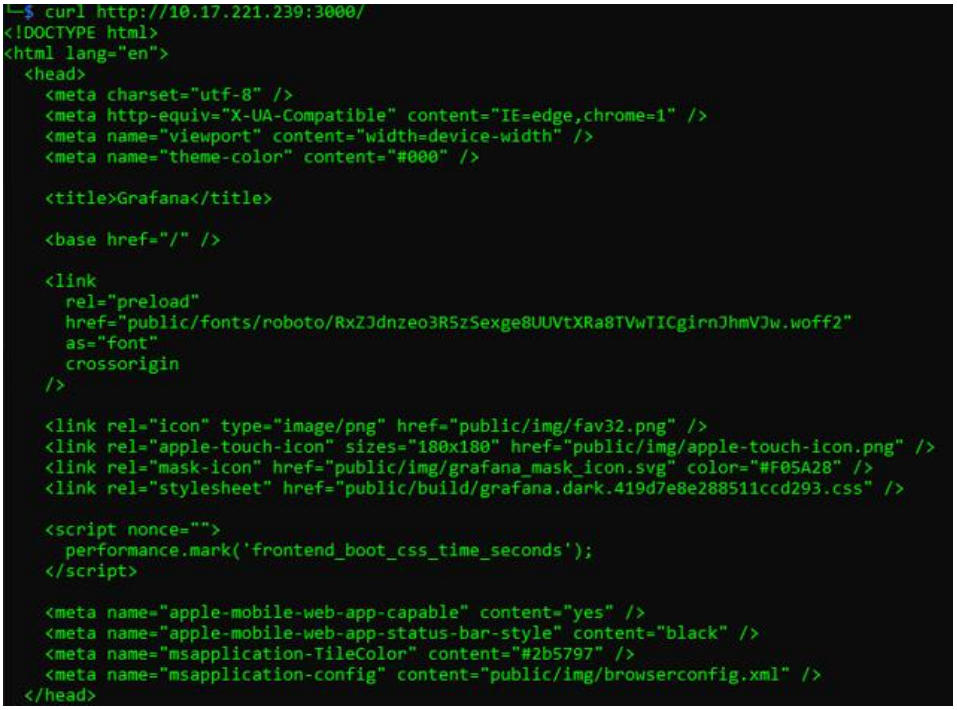

Рисунок 3.10 – Виконання команди “curl” на цільовий сервер

Для усунення вразливості потрібно увійти повернути налаштування за умовчаванням.

ВИСНОВКИ

Кількість і рівень загроз безпеці програмних систем та інформаційних систем від зовнішніх і внутрішніх джерел загроз продовжує зростати. Це пов'язано зі стрімким розвитком засобів обчислювальної і телекомунікаційної техніки, глобальних інформаційних систем, необхідністю розробки для них комплексного програмного забезпечення з використанням сучасних засобів автоматизації процесу проектування програм. Крім того, це пов’язано зі значним або навіть різким зростанням останнім часом активності хакерів і хакерських груп, які атакують інформаційну систему, злочинних груп комп’ютерних зловмисників, різноманітних спеціальних підрозділів і служб, які діють для створення інструментів критичного впливу на вразливі об’єкти. комп'ютеризація. Метою роботи був аналіз сучасних мережевих атак та розробка рекомендацій щодо їх усунення.

Під час виконання дипломної роботи було проведено аналіз можливих загроз на інформаційну безпеку користувачів Інтернет-сервісів. Взято до уваги основні інтернет-послуги, а також деструктивні фактори, існуючі в мережі, та наслідки їх руйнівного впливу. Розглянуті класифікації, наведені описи та характеристики поширені віруси.

Наведено результати порівняльного аналізу останніх версій. Сучасні антивірусні програми за різними критеріями. Дані описи та схеми підключення брандмауерів, принципи роботи робота основних протоколів, що використовуються для захисту інформації та ПК.

Були розглянуті різні системи SIEM, наприклад лідери ринку, і не дуже популярні. До впровадження SIEM рішень, система генерувала сотні тисяч подій на день, обробляючи що було не під силу розпоряднику інформації безпека, однак, після встановлення системи збору та кореляції події інформаційної безпеки кількість подій знизився до десятків на добу. Крім того,

події кількох джерела обробляються за певною схемою, що допомагає виявити інші порушення та інциденти.

Ці засоби не дають стовідсоткової гарантії, але в поєднанні, наприклад з машинне навчання, може дуже ефективно протидіяти будь-якому погрози. Для такої роботи створені системи SIEM, їх основне завдання виявлення, своєчасне попередження та можливе усунення діяльності.

Забезпечення інформаційної безпеки на всіх рівнях досягається комплексним підходом, а саме впровадженням організаційних, організаційно–технічних та технічними заходів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Актуальні кіберзагрози: підсумки 2019 року [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru–ru/research/analytics/cybersecurity–threatscape–2021/#id9.

2. Соціальної інженерії [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://eset.ua

3 7 рад по підвищенню безпеки додатків [Електронний ресурс]. – 2021. – Режим доступу до ресурсу:

https://www.securitylab.ru/analytics/474589.php

4 18 способів захистити ваші онлайн–акаунти від злому [Електронний ресурс] – Режим доступу до ресурсу:

https://revolverlab.com/18–ways–to–make–your–online–accounts–more–secure–3678e64f7e6

5. Навчальний посібник Internet для користувача частина 2, НУДПСУ [[Електронний ресурс] – Режим доступу до ресурсу: https://ua.kursoviks.com.ua/metodychni_vkazivky

6. Правила розмежування доступу [Електронний ресурс] – Режим доступу до ресурсу: https://helppiks.org/6–26934.html.

7. Таненбаум Е. Комп'ютерні мережі [Книга]. – СПб. : Пітер, 2003. – 4–е видання.750 с

8. Рябко Б.Я., Фіона А.Н. Криптографічні методи захисту інформації: [Книга]. М .: Изд–во Гаряча лінія – Телеком, 2005. 336 с

9. Хорошко В.О., Чекатков А.А. Методи і засоби захисту інформації. Україна: Изд–во Юніор, 2003. 504 с

10. SSL certificates [Електронний ресурс] – Режим доступу до ресурсу: https://www.digicert.com/ssl/.

11. SSH (Secure Shell) protocol [Електронний ресурс] – Режим доступу до ресурсу: https://www.ssh.com/ssh/.

12. IPSec – протокол захисту мережевого трафіку на IP–рівні [Електронний ресурс] – Режим доступу до ресурсу: https://www.ixbt.com/comm/ipsecure.shtml

13 X.509 [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/346798/

14 Layer 2 Forwarding (L2F) [Електронний ресурс] – Режим доступу до ресурсу: https://networkencyclopedia.com/layer–2–forwarding–l2f/

15 Point–to–Point Tunneling Protocol (PPTP) [Електронний ресурс] – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc2637