Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістр

студента *Циганова Олександра Олеговича*

академічної групи *125м-22-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Застосування методів цифрової криміналістики при розслідувані інцидентів кібербезпеки на об'єктах критичної інфраструктури*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи				
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Пілова Д.П.	90	Відмінно	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:

завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Циганову Олександру Олеговичу* **академічної групи** *125м-22-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Застосування методів цифрової криміналістики при розслідувані інцидентів кібербезпеки на об'єктах критичної інфраструктури***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.2023р. № 1227-с

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати сучасні загрози для критичної інфраструктури, потенційні наслідки від успішних атак на її мережі і вузли, а також існуючі методи цифрової криміналістики та інциденти, у випадку яких вони використовуються.	28.10.2023
Розділ 2	Описати процес створення тестового полігону з двох docker-контейнерів, на якому в подальшому інсценовати інцидент кіберзпеки. За мотивами змодельованого інциденту провести розслідування методами цифрової криміналістики, відновити картину подій, що сталися, зібрати доказову базу та надати інструкції щодо нейтралізації наслідків інциденту.	16.11.2023
Розділ 3	Розрахувати капітальні витрати на впровадження практики розслідування цифрових злочинів та терміну окупності інвестицій.	08.12.2023

Завдання видано _____ Вадим МЄШКОВ
(підпис керівника) (ім'я, прізвище)

Дата видачі: 16.10.2023 р.

Дата подання до екзаменаційної комісії: 14.12.2023 р.

Прийнято до виконання _____ Олександр ЦИГАНОВ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 83 с., 24 рис., _1_ табл., 4 додатків, 19 джерел.

Об’єкт дослідження - інцидент інформаційної безпеки.

Предмет дослідження - розслідування інцидентів інформаційної безпеки засобами цифрової криміналістики.

Мета кваліфікаційної роботи - дослідити наявні методи цифрової криміналістики і обрати комплексне рішення для розслідування інциденту.

За допомогою обраних методів зібрати доказову базу, описати інцидент, що стався і запропонувати план дій щодо усунення наслідків інциденту.

В першому розділі проаналізовано сучасні загрози для критичної інфраструктури, потенційні наслідки від успішних атак на її мережі і вузли, а також існуючі методи цифрової криміналістики розслідування інцидентів.

У спеціальному розділі було описано процес створення тестового полігону з двох docker-контейнерів, на якому в подальшому проведено моделювання інциденту кібербезпеки. За мотивами змодельованого інциденту було проведено розслідування методами цифрової криміналістики, відновлено картину подій, що сталися, зібрано доказову базу та надано інструкції щодо нейтралізації наслідків інциденту.

В економічному розділі було проведено розрахунки капітальних витрат на впровадження практики розслідування цифрових злочинів та терміну окупності інвестицій.

Наукова новизна полягає в застосуванні методів цифрової криміналістики для розслідування інциденту та наведення плану щодо усунення наслідків інциденту.

ЗАХИСТ ІНФОРМАЦІЇ, ЦИФРОВА КРИМІНАЛІСТИКА, РИЗИКИ, РЕКОМЕНДАЦІЇ.

ABSTRACT

Explanatory note: 83 p., 24 pic., 1 tabl., 4 app., 19 sources.

The object of the study is an information security incident.

The subject of the study is the investigation of information security incidents using digital forensics.

The purpose of the qualification work is to investigate the existing methods of digital forensics and choose a comprehensive solution for investigating the incident.

Using the selected methods, collect evidence, describe the incident and propose an action plan to eliminate the consequences of the incident.

The first section analyzes modern threats to critical infrastructure, the potential consequences of successful attacks on its networks and nodes, as well as existing methods of digital forensics of incident investigation.

In a special section, the process of creating a test site from two docker containers was described, on which a simulation of a cybersecurity incident was subsequently carried out. Based on the simulated incident, an investigation was conducted using digital forensics methods, the picture of the events that occurred was restored, the evidence base was collected and instructions were provided to neutralize the consequences of the incident.

In the economic section, calculations of capital costs for the introduction of digital crime investigation practices and the payback period of investments were carried out.

The scientific novelty is the application of digital forensics techniques to investigate an incident and guide a plan to address the consequences of the incident.

INFORMATION SECURITY. DIGITAL FORENSICS. RISKS. RECOMMENDATIONS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВМ - віртуальна машина

ІКТ - інформаційно-комунікаційні технології

КІ - критична інфраструктура.

ПЗ - програмне забезпечення

ПК - персональний комп'ютер.

DOS (deny of service) - атака типу відмова в обслуговуванні, коли сервіс, на який здійснюється атака стає недоступним на деякий час.

SQL Structured Query Language) - мова запитів, яка використовується для взаємодії з реляційними базами даних.

SSH (secure shell) - протокол, який дозволяє віддалено підключатися до серверу або ПК.

XSS (Cross-Site Scripting) - це тип атаки на веб-додатки, при якій зловмисники вбудовують в веб-сторінки вредливий JavaScript-код.

ЗМІСТ

ВСТУП

В сучасному світі зростає загроза кібербезпеці і об'єкти критичної інфраструктури стають особливо вразливими перед цими загрозами. Забезпечення надійності та стійкості цих об'єктів є важливою завданням для національної безпеки і економіки країни. Інциденти кібербезпеки на таких об'єктах можуть мати серйозні наслідки, включаючи припинення нормального функціонування критичної інфраструктури та втрату конфіденційності критичних даних. Тому розслідування таких інцидентів є доволі важливим завданням.

Застосування цифрової криміналістики у розслідуванні інцидентів кібербезпеки на об’єктах критичної інфраструктури надає можливість збирати, аналізувати та інтерпретувати цифрові сліди, які залишають злочинці під час кібератак. Це допомагає виявити злочинців, встановити мотиви їх дій та надати необхідну доказову базу для їхнього переслідування та покарання. Завдяки цифровій криміналістиці можливо зберегти нормальне функціонування об'єктів критичної інфраструктури та запобігти подібним інцидентам у майбутньому.

Спеціалісти в галузі цифрової криміналістики мають безпосередній зв'язок з розслідуванням інцидентів кібербезпеки на об'єктах критичної інфраструктури. Вони володіють необхідними знаннями та навичками для здійснення цифрового аналізу, виявлення слідів кіберзлочинів та забезпечення їхнього відновлення. Таким чином, робота з об'єктами критичної інфраструктури вимагає високого рівня професіоналізму у сфері цифрової криміналістики.

Серед великої різноманітності методів цифрової криміналістики, важливо вміти оперативно визначати найефективніші для розслідування конкретного інциденту, ця навичка є запорукою результативності розслідування будь-якого злочину і підвищення захищеності цифрової інфраструктури.

Метою даної кваліфікаційної роботи стало дослідити наявні методи цифрової криміналістики і обрати найоптимальніші для розслідування змодельованого інциденту. З допомогою обраних методів зібрати доказову базу, відновити картину того, що відбулося і запропонувати план дій щодо усунення наслідків інциденту.. Головні задачі включають:

1. Обрати одну з найпоширеніших типів вразливостей;
2. В тестовому середовищі розгорнути завідома вразливий сервіс;
3. Змоделювати поведінку злочинця шляхом експлуатації вразливості;
4. Провести розслідування змодельованого інциденту використовуючи методи цифрової криміналістики, зібрати доказову базу:
5. Створити план, щодо усунення наслідків інсценованого інциденту.

1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Критична інфраструктура

Об'єкти критичної інфраструктури - підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв.

Закон України «Про основні засади забезпечення кібербезпеки України» використовує термін «Критично важливі об'єкти інфраструктури», визначаючи їх як юридичні особи, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Цей Закон також надає взаємопов'язане визначення об'єкт критичної інформаційної інфраструктури: комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури.

Європейський Союз визначає критичну інфраструктуру як системи, які мають важливе значення для підтримки життєво важливих соціальних функцій. Пошкодження критичної інфраструктури, її руйнування або порушення в результаті стихійних лих, тероризму, злочинної діяльності або зловмисної поведінки, може істотно негативно вплинути на безпеку ЄС і добробут громадян. [1]

Згідно ст. 8 Закону України «Про критичну інфраструктуру»

Віднесення об’єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму.

До таких критеріїв належать:

1) виконання функцій із забезпечення життєво важливих національних інтересів;

2) існування викликів і загроз, що можуть виникати щодо об’єктів критичної інфраструктури;

3) ймовірність завдання значної шкоди нормальним умовам життєдіяльності населення;

4) уразливість таких об’єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода здоров’ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); державному суверенітету (зниження обороноздатності, дискредитація іміджу країни, дестабілізація системи державного управління та унеможливлення виконання державою своїх функцій); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення;

5) масштабність негативних наслідків для держави, які впливають на діяльність стратегічно важливих об’єктів для кількох секторів життєзабезпечення чи призводять до втрати унікальних національно значущих активів, систем і

ресурсів, матимуть тривалі наслідки для держави і позначаться на діяльності ряду інших секторів;

6) тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави;

7) вплив на функціонування суміжних секторів критичної інфраструктури.

Згідно ст. 9 Закону України «Про критичну інфраструктуру» до життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема:

1) урядування та надання найважливіших публічних (адміністративних) послуг;

2) енергозабезпечення (у тому числі постачання теплової енергії);

3) водопостачання та водовідведення;

4) продовольче забезпечення;

5) охорона здоров'я;

6) фармацевтична промисловість;

7) виготовлення вакцин, стале функціонування біолабораторій;

8) інформаційні послуги;

9) електронні комунікації;

10) фінансові послуги;

11) транспортне забезпечення;

12) оборона, державна безпека;

13) правопорядок, здійснення правосуддя, тримання під вартою;

14) цивільний захист населення та територій, служби порятунку;

15) космічна діяльність, космічні технології та послуги;

16) хімічна промисловість;

17) дослідницька діяльність.

Згідно ст. 22 Закону України «Про критичну інфраструктуру» на державному рівні розробляється Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури, який затверджується Кабінетом Міністрів України.

На секторальному (галузевому) та регіональному рівнях органи державної влади розробляють і затверджують галузеві, регіональні плани та програми з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань.

Національна поліція України, Національна гвардія України, Служба безпеки України, Збройні Сили України, Державна служба України з питань надзвичайних ситуацій та інші складові сектору безпеки і оборони у межах компетенції здійснюють планування відповідних заходів із захисту критичної інфраструктури.

На місцевому рівні: місцеві органи виконавчої влади (військово-цивільні адміністрації - у разі утворення), органи місцевого самоврядування забезпечують розроблення, затвердження і виконання місцевих програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням надання чи погіршенням якості важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій. Такі програми включають заходи із забезпечення безпеки та стійкості критичної інфраструктури, взаємодії суб'єктів національної системи захисту критичної інфраструктури, а також відновлення функціонування об'єктів критичної інфраструктури.

На об'єктовому рівні: оператори критичної інфраструктури на кожному об'єкті критичної інфраструктури розробляють та забезпечують виконання об'єктового плану заходів щодо захисту і забезпечення стійкості критичної інфраструктури, який включає заходи з фізичного захисту, протидії загрозам, ефективного зниження та контролю за ризиками безпеки, забезпечення безпеки інформації та кібербезпеки на об'єктах критичної інфраструктури.

Плани та програми, затверджені відповідно до цієї статті, є обов'язковими до виконання всіма суб'єктами національної системи захисту критичної інфраструктури. [2]

1.2. Захист України в кіберпросторі

Кіберполіція (Департамент кіберполіції Національної поліції України) - міжрегіональний територіальний орган Національної поліції України, який входить

до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем.

Основними завданнями Кіберполіції є:

1. Реалізація державної політики у сфері протидії кіберзлочинності.
2. Завчасне інформування населення про появу новітніх кіберзлочинів.
3. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.
4. Реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.
5. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.
6. Участь у міжнародних операціях та співпраця в режимі реального часу.
7. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.
8. Протидія кіберзлочинам.[3]

1.3. Загроза кібератак на КІ і їх потенційні наслідки.

З 2014 року Російська Федерація активно використовує кіберпростір у гібридній агресії проти України шляхом здійснення деструктивного впливу на органи державної влади, системи управління військами та зброєю сил оборони, а також на об’єкти критичної інфраструктури. Держава-агресор невпинно нарощує арсенал кіберзброї наступального, розвідувального та підривного призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Зазначені чинники вимагають постійного нарощування можливостей забезпечення кібербезпеки органами сектору безпеки і оборони.

Надзвичайно актуальною загрозою на сьогодні є розвідувально-підривна діяльність у кіберпросторі проти України, яка пов'язана з проведенням спецслужбами іноземних держав, насамперед Російської Федерації, розвідувальної діяльності з метою викрадення інформації (кібершпигунство) та підривних акцій з порушення штатного режиму функціонування об'єктів критичної інформаційної інфраструктури, передусім систем управління державою, об'єктів життєзабезпечення, електроенергетики, транспорту, ядерної і хімічної промисловості, банківської сфери (актів кібердиверсій).

В Україні в останні роки відчутно зросла загроза кібертероризму. Насамперед, це пов'язано з кіберможливостями держави-агресора Російської Федерації, яка веде проти України кібервійну із застосуванням кіберзброї. Спостерігається використання кіберпростору для фінансування терористичних угруповань. Водночас недостатньою є взаємодія України з міжнародними партнерами щодо опрацювання на взаємовигідній основі механізмів протидії кібертероризму.

Зростання кіберзлочинності в національному сегменті кіберпростору є масштабною загрозою, яка завдає шкоди державним інформаційним ресурсам, суспільним процесам, особисто громадянам, що знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення інших злочинів (проти основ національної безпеки, легалізації доходів, одержаних злочинним шляхом, торгівлі людьми, незаконного обігу зброї, наркотичних засобів та інших предметів і речовин, які загрожують життю та здоров'ю людей). Ситуація ускладняється через низький рівень кіберграмотності населення, зокрема пересічних користувачів електронних послуг.

Державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури, які призначені для забезпечення задоволення життєво важливих потреб громадянина, особи, суспільства і держави, є недостатньо захищеними від кібератак.

Державні органи, приймаючи рішення про автоматизацію процесів державного управління, не завжди оцінюють ризики, що виникають у кіберзахисті державних

інформаційних ресурсів. Захист інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина службової інформації та персональних даних громадян, не відповідає вимогам законодавства, що посилює ризики втручання в такі системи, загрожує конфіденційності, цілісності та доступності інформації (реєстри, бази даних), яка призначена для задоволення потреб та забезпечення конституційно гарантованих інтересів, громадян, суспільства і держави.

Висока технологічна залежність України від іноземних виробників продукції ІКТ та програмного забезпечення управління нею, відсутність сучасних національних стандартів щодо вимог з безпеки ланцюга поставок відповідного обладнання, розроблення програмного забезпечення та інформаційно-комунікаційних систем, систем сертифікації або оцінки відповідності з безпеки такої продукції підвищують ступінь уразливості об'єктів військової, політичної, фінансово-економічної та промислової інфраструктури держави від шкідливих і незадекларованих функцій у такому обладнанні та звужують вітчизняні спроможності протидії кіберзагрозам.

Значна частина підприємств, установ та організацій усіх форм власності не забезпечують кіберзахист електронних інформаційних ресурсів, якими вони розпоряджаються, що призводить до порушень прав користувачів цифрових послуг та дискредитує процеси цифрової трансформації в державі.

Базовий ландшафт інструментарію реалізації окреслених кіберзагроз характеризується зростанням високотехнологічної складової та різноманіттям.

Безперервно збільшується кількість кібератак, спрямованих на викрадення персональних та інших конфіденційних даних громадян та організацій із використанням методів соціальної інженерії.

Зростає рівень ризику застосування фішингових атак, ботнетів, шкідливого програмного забезпечення, у тому числі програм-вимагачів, як з боку фінансово мотивованих кіберзлочинних груп, так і з боку хакерських угруповань, підконтрольних країні-агресору та іншим країнам.

Збільшення інформації у базах даних та інформаційних системах та посилення відповідальності за витоки персональних даних громадян у провідних країнах створило глобальний ринок для розвитку програм-вимагачів, які вимагають кошти за розблокування доступу до інформації або нерозміщення викраденої інформації в мережі Інтернет.

Усе частіше спрямовані кібератаки не здійснюються напряму на уряди та організації. Кібератак зазнають розробники та постачальники програмних і апаратних засобів з метою зараження популярних додатків, внесення змін у вихідні коди та процеси оновлень. У подальшому це використовується для проникнення до великої кількості їх клієнтів та завдання масштабної шкоди.

Популярні веб-сайти, соціальні мережі, реєстри збирають велику кількість ідентифікаційних та персональних даних користувачів. Витоки інформації з баз даних, які їм належать, створюють загрозу використання цих даних з метою атаки на інші ресурси та інформаційні системи.

Передумови та чинники, які формують окреслені загрози:

– недосконалість нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня урегульованість цифрової складової частини розслідування злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

– відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом. Фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;

– відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі;

– відсутність законодавчого акту про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

– незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

– відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту. [4]

1.4. Огляд сучасних типів кібератак. Необхідність аналізу і досліджень сучасних методів атаки на критичну інфраструктуру.

Кіберзлочинність різко зростає з кожним роком, оскільки зловмисники покращують свою ефективність і витонченість. Кібератаки відбуваються з різних причин і різними способами. Однак загальним є те, що кіберзлочинці намагатимуться використати вразливі місця в політиках безпеки, практиках або технології організації.

Кібератака - це спроба зловмисника отримати неавторизований доступ до IT-системи з метою крадіжки, вимагання, збою або з інших нечесних причин.

Звичайно, велика кількість інцидентів безпеки спричинена інсайдерами - через недбалість чи злочинний умисел. Однак для простоти припустімо, що кібератаку здійснив хтось, хто не є або не був членом організації.

Хоча зловмисник може проникнути в IT-систему різними способами, більшість кібератак покладаються на досить схожі методи. Нижче наведено деякі з найпоширеніших типів кібератак:

1. Шкідливе ПЗ
2. Фішинг
3. Атака "людина посередині" (MITM)

4. Розподілена атака на відмову в обслуговуванні (DDoS).
5. SQL ін'єкція
6. Експлуатація вразливостей нульового дня
7. Тунелювання DNS
8. Компрометація корпоративної-електронної пошти (BEC)
9. Криптоджекінг (Cryptojacking)
10. Drive-by Attack
11. Міжсайтовий скриптинг (XSS)
12. Атака на паролі
13. Підслуховування (Eavesdropping)
14. Внутрішні загрози (Insider Threats)
15. Атаки на пристрої Інтернету речей

1.4.1. Шкідливе ПЗ

Шкідливе ПЗ або зловмисне ПЗ - це небажане ПЗ, яке встановлюється у вашій системі без вашого дозволу. Воно може ховатися на законних вебсайтах і програмах або приєднуватися до файлів. Різні типи зловмисного програмного забезпечення мають різні методи зараження та шкоди комп'ютеру, наприклад, реплікація, шифрування файлів, блокування доступу до даних, показ реклами або таємний збір інформації. Різні типи шкідливих програм включають:

Віруси - це шкідливі програми, які розмножуються та заражають інші файли та системи.

Черв'яки - черв'яки схожі на віруси, але вони можуть поширюватися незалежно, не приєднуючись до інших файлів або програм.

Трояни - трояни маскуються під законне програмне забезпечення, обманом змушуючи користувачів їх встановити.

Програми-вимагачі - програми-вимагачі шифрують файли на комп'ютері жертви та вимагають викуп за відновлення доступу до них.

Шпигунське ПЗ - шпигунське програмне забезпечення призначене для таємного збору інформації про дії користувача, зазвичай без його відома чи згоди.

Він може фіксувати натискання клавіш, контролювати звички перегляду та збирати особисту інформацію.

Рекламне ПЗ - рекламне ПЗ відображає небажану рекламу на пристрої користувача. Хоча це не завжди шкідливо, воно може бути нав'язливим і негативно впливати на продуктивність системи.

Кейлогери - фіксують і записують натискання клавіш на комп'ютері, дозволяючи зловмисникам збирати конфіденційну інформацію, як-от паролі, дані кредитної картки та облікові дані для входу.

Руткіти - це складне шкідливе програмне забезпечення, призначене для отримання несанкціонованого доступу до комп'ютерної системи та маскування присутності інших шкідливих програм.

Бот-нет - це мережі скомпрометованих комп'ютерів, підключених до центрального командного сервера. Зловмисники використовують ці мережі для здійснення різноманітних зловмисних дій, таких як запуск розподілених атак типу «відмова в обслуговуванні» (DDoS) або розсилання спаму.

Безфайлове зловмисне програмне забезпечення - цей тип зловмисного програмного забезпечення не покладається на традиційні файли для зараження системи. Натомість він зберігається в пам'яті або реєстрі пристрою, що ускладнює його виявлення та видалення.

Це лише деякі з багатьох типів зловмисного програмного забезпечення, і нові варіанти постійно розробляються, оскільки зловмисники вдосконалюють свою тактику.

Одним із найвідоміших прикладів зловмисного програмного забезпечення є Emotet, який спричинив значні фінансові збитки та збитки для окремих осіб, організацій та урядів. Emotet виник як банківський троян у 2014 році, але з тих пір перетворився на модульну та поліморфну шкідливу програму, через що її надзвичайно важко виявити та знищити. Emotet в основному поширюється через вміло створені фішингові електронні листи, що містять зловмисні додатки або шкідливі посилання, натискання яких запускає потоки шкідливих корисних даних. Якщо систему жертви скомпрометовано, Emotet прописує себе в системі та може

діяти непоміченим, викрадаючи конфіденційні дані, поширюючи їх на інші пристрої в мережі та навіть доставляючи додаткові шкідливі програми.

1.4.2. Фішинг

Фішинг - це форма кібератаки, яка передбачає використання електронної пошти, SMS, телефонних дзвінків, соціальних мереж і методів соціальної інженерії, щоб обманом змусити жертв розкрити конфіденційну інформацію або завантажити шкідливі файли, які можуть заразити їхні пристрої.

Типи фішингових атак:

1. Spear Phishing - це цілеспрямована атака, спрямована на конкретних осіб або організації. Він передбачає надсилання шахрайських електронних листів, призначених для отримання цінної інформації або зараження пристрою одержувача шкідливим програмним забезпеченням

2. Вейлінг (англ. Whaling) - спрямовані саме на високопоставлених керівників або старших службовців. Мета - викрасти гроші або конфіденційну інформацію та отримати несанкціонований доступ до їхніх систем для подальших кібератак.

3. Смішинг (англ. SMiShing) - це спосіб обману, який передбачає надсилання шахрайських текстових повідомлень. Мета полягає в тому, щоб спонукати людей розкрити конфіденційні дані, такі як паролі, імена користувачів і номери кредитних карток. Кіберзлочинці часто видають себе за довірені організації, такі як банки чи служби доставки.

4. Вішинг (англ. Vishing) відноситься до голосового фішингу, коли шахраї використовують телефонні дзвінки та голосові повідомлення, щоб видавати себе за авторитетні організації. Вони маніпулюють особами, змушуючи їх розкривати особисту інформацію, як-от банківські реквізити та паролі.

1.4.3. MiTM - Man in the Middle attack (англ. атака типу «Людина посередені»)

Атака «людина посередині» (MITM) - це ситуація, коли зловмисник перехоплює зв'язок між двома сторонами, намагаючись шпигувати за жертвами, викрасти особисту інформацію чи облікові дані чи, можливо, якимось чином змінити розмову. Атаки MITM сьогодні менш поширені, оскільки більшість систем електронної пошти та чату використовують наскрізне шифрування, яке запобігає

втручанню сторонніх осіб у дані, які передаються через мережу, незалежно від того, безпечна мережа чи ні.

1.4.4. Атака типу «Відмова в обслуговуванні» або DoS/DDoS

Метою DoS-атаки є перевантаження ресурсів системи, через що вона не може відповідати на легітимні запити на обслуговування. DDoS-атака схожа, але залучає кілька заражених зловмисним програмним забезпеченням хостів, якими керує зловмисник. Ці атаки перешкоджають належному функціонуванню цільового сайту та можуть призвести до повного вимкнення. На відміну від інших кібератак, які приносять безпосередню користь хакерам, атаки DoS і DDoS просто спрямовані на порушення роботи цільових служб. Однак у деяких випадках зловмисник може отримати фінансову вигоду, якщо його найме бізнес-конкурент. Успішні атаки DoS або DDoS можуть зробити систему вразливою до інших типів атак.

У лютому 2020 року велика DoS-атака була спрямована на Amazon Web Services (AWS). Вважалося, що ця атака була найбільшою DDoS-атакою в історії, хоча інші стверджували, що це була лише найбільша оприлюднена DDoS-атака. Наприклад, у вересні 2016 року експерт з кібербезпеки Браян Кребс зазнав масової DDoS-атаки на свій блог із навантаженням трафіку понад 620 Гбіт/с. Ця атака, здійснена ботнетом Mirai, була майже втричі масштабнішою за будь-які попередні атаки. Ботнет Mirai складався зі зламаних пристроїв IoT і був виявлений місяцем раніше. Невдовзі після цього ботнет атакував великого європейського хостинг-провайдера OVH, який тривав сім днів і створював трафік до 1,1 терабіт на секунду. OVH був не єдиною жертвою ботнету Mirai того року.

1.4.5. SQL-ін’єкції

SQL-ін’єкція - це тип атаки, характерний для баз даних SQL. Бази даних SQL використовують оператори SQL для запиту даних, і ці оператори зазвичай виконуються через форму HTML на веб-сторінці. Якщо дозволи бази даних не встановлено належним чином, зловмисник може використати форму HTML для виконання запитів, які створюватимуть, читатимуть, змінювати або видаляти дані, що зберігаються в базі даних.

1.4.6. Експлуатація Zero-day вразливостей

Експлойт нульового дня - це коли кіберзлочинці дізнаються про вразливість, яка була виявлена в певних широко використовуваних програмних додатках та операційних системах, а потім націлюються на організації, які використовують це програмне забезпечення, щоб використати вразливість до того, як стане доступним виправлення.

1.4.7. Тунелювання DNS

Тунелювання DNS - це складний вектор атаки, який призначений для надання зловмисникам постійного доступу до заданої цілі. Оскільки багато організацій не можуть відстежувати DNS-трафік на предмет зловмисної активності, зловмисники можуть вставляти або «тунелювати» шкідливе програмне забезпечення в DNS-запити (DNS-запити, що надсилаються від клієнта до сервера). Зловмисне програмне забезпечення використовується для створення постійного каналу зв'язку, який більшість брандмауерів не можуть виявити.

1.4.8. Компрометація корпоративної поштової скриньки (BEC)

Атака BEC (Business Email Compromise) - це тип атаки, коли зловмисник націлений на конкретних осіб, як правило, на співробітника, який має можливість авторизувати фінансові транзакції, щоб обманом змусити їх переказати гроші на рахунок, контрольований зловмисником. Атаки BEC, як правило, включають планування та дослідження, щоб бути ефективними. Наприклад, будь-яка інформація про керівників цільової організації, співробітників, клієнтів, ділових партнерів і потенційних ділових партнерів допоможе зловмиснику переконати співробітника передати кошти. Атаки BEC є однією з найбільш фінансово руйнівних форм кібератак.

1.4.9. Криптоджекінг

Криптоджекінг (cryptojacking) - це коли кіберзлочинці компрометують комп'ютер або пристрій користувача та використовують його для майнінгу криптовалют, таких як біткойн. Криптоджекінг не так відомий, як інші вектори атак, однак його не слід недооцінювати. Організації не мають великої видимості, коли справа доходить до цього типу атаки, а це означає, що хакер може

використовувати цінні мережеві ресурси для майнінгу криптовалюти, не знаючої про це організації. Звичайно, вимивання ресурсів з мережі компанії є набагато менш руйнівними, ніж крадіжка цінних даних.

1.4.10. Drive-by атаки

Атака «drive-by-download» - це коли нічого не підозрююча жертва відвідує вебсайт, який, у свою чергу, заражає її пристрій шкідливим програмним забезпеченням. Вебсайт, про який йде мова, може бути таким, який безпосередньо контролюється зловмисником, або таким, який був скомпрометований. У деяких випадках зловмисне програмне забезпечення подається в такому вмісті, як банери та реклама. Сьогодні доступні набори експлойтів, які дозволяють хакерам-початківцям легко налаштовувати шкідливі вебсайти або поширювати шкідливий вміст іншими способами.

1.4.11. Атаки міжсайтового скриптингу (XSS)

Атаки міжсайтового скриптингу дуже схожі на атаки SQL-ін'єкцій, хоча замість вилучення даних з бази даних вони зазвичай використовуються для зараження інших користувачів, які відвідують сайт. Простим прикладом може бути розділ коментарів на вебсторінці. Якщо введені користувачем дані не відфільтрувати перед публікацією коментаря, зловмисник може опублікувати шкідливий сценарій, прихований на сторінці. Коли користувач відвідує цю сторінку, скрипт виконується і або заражає його пристрій, або використовується для крадіжки файлів cookie, або, можливо, навіть використовується для вилучення облікових даних користувача. Крім того, вони можуть просто перенаправити користувача на шкідливий вебсайт.

1.4.12. Атаки на паролі

Атака на паролі, це різновид кібератаки, коли зловмисник намагається вгадати або «зламати» пароль користувача. Існує багато різних методів злому пароля користувача, хоча пояснення цих різних методів виходить за рамки цієї статті. Однак деякі приклади включають атаку грубої сили, атаку за словником, атаку за райдужною таблицею, атаку кейлоггера і банато. інших. І, звичайно, зловмисники

часто намагаються використовувати методи фішингу, щоб отримати пароль користувача.

1.4.13. Підслуховування

Атака прослуховування, яку іноді називають «стеженням» або «сніфінгом», полягає в тому, що зловмисник шукає незахищені мережеві зв'язки, намагаючись перехопити та отримати доступ до даних, які надсилаються мережею. Це одна з причин, чому співробітників просять використовувати VPN при доступі до мережі компанії з незахищеної загальнодоступної точки доступу Wi-Fi.

1.4.14. Insider Threats

IT-команди, які зосереджуються виключно на виявленні зовнішніх зловмисників, отримують лише часткове розуміння загального ландшафту загроз. Внутрішні загрози, які складаються з нинішніх або колишніх співробітників, становлять значну небезпеку для організацій через їх необмежений доступ до мережі компанії, включаючи конфіденційні дані та інтелектуальну власність. Їх обізнаність з бізнес-процедурами, політикою компанії та іншою відповідною інформацією, яка може допомогти в проведенні атаки.

Внутрішні суб'єкти, які наражають на небезпеку організацію, як правило, мають злі наміри. Їхня мотивація може полягати в отриманні грошової вигоди шляхом продажу конфіденційної інформації в даркнеті. І навпаки, деякі суб'єкти внутрішніх загроз демонструють недбалість, а не зловмисність. Щоб протидіяти цій проблемі, організації повинні створити комплексну навчальну програму з кібербезпеки, яка інформує всі зацікавлені сторони про можливі загрози, включаючи ті, які можуть походити зсередини організації.

1.4.15. Атаки на прилади інтернету речей

Пристрої IoT (internet of Things), як правило, взаємопов'язані, а це означає, що якщо один пристрій буде скомпрометовано, можливо, атака поширеться на інші пристрої. Що ще гірше, пристрої IoT майже не мають вбудованого захисту, що робить їх ідеальною мішенню для зловмисників. На додаток до впровадження загальних заходів безпеки, потрібно переконатися, що налаштування маршрутизатора за замовчуванням було змінено, встановлено надійний і

унікальний пароль, пристрої IoT відключені, коли вони не використовуються, і переконатися, що на них встановлені останні виправлення/оновлення.[5]

1.5. Роль цифрової криміналістики в аналізі і дослідженнях кібератак і злоякісного ПЗ.

Цифрова криміналістика - це галузь криміналістики, яка займається відновленням, розслідуванням і збереженням цифрових доказів, дотримуючись правових стандартів.

Очікується, що до 2028 року світова криміналістична індустрія принесе близько 27,7 мільярдів доларів США, згідно зі звітом Vantage Market Research про ринок криміналістичних технологій за 2022 рік. Ця цифра має сенс з огляду на постійний, динамічний технологічний прогрес у світі.

«Комп'ютерна криміналістика» була першим терміном, який використовувався для розслідування злочинів, пов'язаних з комп'ютером. ФБР запустило першу програму комп'ютерної криміналістики в 1984 році, а перша пастка була створена в 1986 році Кліффом Столлом в Національній лабораторії Лоуренса Берклі. Комп'ютерна криміналістика стала професією, головним чином для стримування поширення дитячої порнографії.

Згодом термін «цифрова криміналістика» почав використовуватися для позначення будь-якої технології, яка містить цифрові дані. Ми використовуємо терміни «цифрова криміналістика», «комп'ютерна криміналістика» та «кіберкриміналістика» як синоніми.

Криміналістика, як правило, пов'язана з аналізом будь-якого місця злочину. Наприклад, після пограбування місце злочину прочісують на предмет відбитків пальців і всього іншого, що може привести до доказів ДНК. У цифровій криміналістиці місцем злочину стає пристрій. Слідчий намагається з'ясувати, хто отримав до нього доступ, що на ньому зберігалося, що можна було видалити тощо.

Цифровою криміналістикою в основному користуються дві групи людей:

– Правоохоронні органи у кримінальних та цивільних справах: Ці органи використовують цифрові докази для допомоги підозрюваним у засудженні чи

виправданні. Ці справи можуть варіюватися від судових процесів у справах про вбивство до цивільних справ, наприклад, пов'язаних з передачею майна.

– Групи реагування на інциденти в організаціях: ці команди першими реагують на кібератаки, такі як витік даних або загрози програм-вимагачів. Вони використовують цифрову криміналістику для дослідження точок входу та можливого виправлення.

Конкретні події в корпоративному середовищі ініціюють цифрові криміналістичні розслідування. Ці події включають аномальну активність у мережі або серверах, корпоративне шпигунство, кібератаки, крадіжку інтелектуальної власності, розслідування банкрутства або аудити відповідності галузевим стандартам.

Кінцевою метою кіберкриміналістики є проведення структурованого розслідування на основі керівних принципів, результатом якого є документ. Цей документ повинен бути готовий до використання в якості доказу в суді або в аудиторських органах.

Слідчий з кіберкриміналістики - це експерт зі ступенем бакалавра (або вище) в галузі комп'ютерної криміналістики. Цей фахівець повинен вміти розуміти злочинні наміри і відповідно слідувати слідству.

«Цифрові докази» залежать від типу пристрою, який потрібно проаналізувати. Це може бути що завгодно: від даних облікового запису користувача до електронних дверних журналів. Слідчі можуть збирати два типи цифрових доказів:

– Нестабільні дані - це цифрова інформація, що зберігається на тимчасовому носії. Ці дані втрачаються, коли пристрій вимикається. Найбільш поширеними нестабільними даними в розслідуванні цифрової криміналістики є оперативна пам'ять (ОЗП). Іншими прикладами є мережеві підключення, відкриті файли, запущені процеси та активні сеанси. Зазвичай з цих джерел можна зібрати деякі залишкові дані.

– Енергонезалежні дані - це цифрова інформація, що зберігається на постійних носіях, таких як жорсткі диски. Дані не втрачаються навіть при вимкненому пристрої. Енергонезалежні дані включають системні файли, журнали

подій, файли дампів, файли конфігурації та інформацію про облікові записи. Ці дані менш складно отримати з метою доказування, ніж нестабільні дані.

Інструменти цифрової криміналістики можуть бути апаратними або програмними. Ці інструменти використовуються для перевірки пристроїв, зберігаючи цілісність даних. Деякі стандартні інструменти:

– Інструменти аналізу файлів: ці інструменти витягують і аналізують окремі файли.

– Інструменти мережевого аналізу: Це переважно інструменти моніторингу мережі, які витягують інформацію про трафік і корисне навантаження.

– Аналізатори баз даних: ці інструменти витягують, аналізують і запитують базу даних для збору необхідної інформації.

– Інструменти реєстру: обчислювальні системи на базі Windows підтримують активність користувачів у так званих реєстрах. Ці інструменти збирають з них інформацію.

– Інструменти збору даних: Ці інструменти збирають дані, як зашифровані, так і звичайні. Вони роблять побайтову копію на жорсткі диски та дозволяють витягувати дані без пошкодження оригінального вмісту.

– Сканери електронної пошти: вони сканують усі повідомлення електронної пошти на наявність доказів. Вони важливі для розслідування атак соціальної інженерії.

– Сканери мобільних пристроїв: ці пристрої сканують внутрішню та мобільну пам'ять на мобільних пристроях.

Процес комп'ютерної криміналістики є реактивним - розслідуванням, яке починається після настання події. Він відокремлений від процесу кібербезпеки, який організація повинна включити для загального стану безпеки. Заходи кібербезпеки гарантують, що такі події будуть заздалегідь зведені до мінімуму.

1.5.1. Типи цифрової криміналістики

Комп'ютерна криміналістика починалася як єдина наука. Однак вона розгалужується через різноманітність цифрових даних (рис. 1.1).

Рисунок 1.1 - Типи цифрової криміналістики

Виходячи з спрямованості дослідження, різними видами цифрової криміналістики є:

1. Електронне виявлення - це цифровий аналіз, обробка та збереження даних. Він використовується в нормативному або правовому контексті.

2. Аналіз криміналістичних даних - це тип кіберкриміналістики, який має справу з організованими даними. Він передбачає, що аналітики даних перевіряють носії даних, щоб отримати корисні докази. В основному це стосується сфери фінансового шахрайства.

3. Реагування на інциденти - це цифрова криміналістика з корпоративної точки зору. Цей тип криміналістики спрямований на забезпечення безперервності бізнесу та зменшення впливу події (наприклад, витоку даних). В основному його виконують внутрішні команди в організації.

4. Комп'ютерна криміналістика - це цифрова криміналістика, яка займається доступом, збором та аналізом інформації про комп'ютерні системи, які працюють на обчислювальній потужності або сховищі. Більшість видів цифрової криміналістики є галуззю комп'ютерної криміналістики.

5. Мережева криміналістика. Автономні комп'ютери сьогодні зустрічаються рідко. Практично всі цифрові пристрої з'єднані між собою та інтернетом за допомогою комп'ютерних мереж. Мережева криміналістика передбачає аналіз моделей мережевого трафіку та компрометуючих корисних навантажень.

6. Криміналістика баз даних передбачає аналіз і вилучення даних і метаданих з баз даних. Сюди входять дані, що зберігаються сторонніми службами в договорі з підозрюваним. Це можуть бути навіть постачальники SaaS, якщо розглядати інциденти в організаціях.

7. Дискова криміналістика. Інша підмножина комп'ютерної криміналістики, дискова криміналістика, спеціалізується на пошуку та відновленні даних з енергонезалежних пристроїв.

8. Криміналістика пам'яті. У той час як дискова криміналістика фокусується на постійному зберіганні, криміналістика пам'яті фокусується на оперативній пам'яті. Криміналістику пам'яті також називають роботою на живу, оскільки вона представляє «місце злочину» таким, яким воно є.

9. Криміналістика хмарних сервісів. Оскільки більшість систем зараз працюють у хмарі, хмарна криміналістика має справу з інформацією, розміщеною в хмарі. Для цього потрібен аналіз конфігурації, безпеки та геолокації хмарних активів. Хмарна криміналістика вимагає співпраці з постачальниками хмарних послуг (такими як AWS і Google Cloud).

10. Криміналістика електронної пошти передбачає отримання та сканування всіх повідомлень електронної пошти, включаючи видалені. Аналітики-криміналісти шукають особи, вміст, позначки часу та інші метадані, прикріплені до електронних листів. Криміналістика електронної пошти шукає підроблені електронні листи та шкідливий вміст, наприклад фішингові електронні листи.

11. Криміналістика зловмисного програмного забезпечення - це тип криміналістики, який займається відстеженням джерела шкідливого програмного забезпечення, яке вже було впроваджено в систему. Іноді це частина реагування на інциденти. Криміналістичні аналітики зловмисного програмного забезпечення досліджують ступінь шкоди та намагаються відстежити її до коду, який використовується для створення шкідливого програмного забезпечення.

Більшість цифрових криміналістичних слідчих спеціалізуються більш ніж на одному з цих типів. Тип цифрової криміналістики, що використовується у справі, залежить від наявних доказів і характеру злочину (або інциденту), який повинен розкрити слідчий.

1.5.2. Процес цифрової криміналістики

Цифрова криміналістика, незалежно від типу, вимагає упередженого та системного підходу. Існує кілька моделей цифрових криміналістичних процесів, яких можна дотримуватися. Кроки в кожній з цих моделей різняться залежно від мети розслідування: правоохоронні органи, аудит або реагування на інциденти (рис. 1.2).

Крок 1: Підготовка до розслідування

Це перший етап будь-якого розслідування. Тут слідчі стежать за тим, щоб у них були потрібні інструменти та люди. Зрештою, це залежить від типу події, яка розслідується.

У разі проведення судового розслідування слідча група отримує повноваження на обшук. У кримінальній справі орган обшуку приходить з ордером на обшук або повісткою до суду. У цивільній справі це може бути просто згода на обшук.

Криміналістичні інструменти також перевіряються на цьому етапі. Слідчі повинні очистити кожну одиницю апаратного та програмного забезпечення від проблем і перевірити їх точність. Це особливо важливо для нових і старих інструментів з новими оновленнями або патчами. Іноді може знадобитися повторний етап валідації перед етапом аналізу. Щоразу, коли ця перевірка виконується, її потрібно документувати.

Процеси, про які йшлося вище, мають вирішальне значення. Якщо все зроблено неправильно, це зводить нанівець будь-які висновки розслідування і не може бути використане в суді.

У разі реагування на інциденти групи зовнішніх розслідувань вимагають SLA (угода про рівень обслуговування), тоді як внутрішнім командам просто потрібно встановити свій ланцюжок командування. Як тільки це буде зроблено, створюється список можливих цифрових пристроїв і систем. Це робиться шляхом пошуку цифрового сліду.

Рисунок 1.2 - Схема процесу цифрової крміналістики

Цифровий слід відстежує діяльність. Наприклад, у справі про крадіжку інтелектуальної власності слідчі з'ясовують поведінку підозрюваного в системі. Це включає програми, до яких вони отримували доступ, які вебсайти вони відвідували та які пристрої використовували. Відстеження цифрового сліду створює список

активів. Потім пункти цього списку вилучаються для глибокого аналізу, пам'ятаючи про злочинний намір.

Крок 2: Ідентифікація доказів

Після того, як початкові деталі та законність визначені, другим кроком є ідентифікація доказів і з'ясування, де вони зберігаються.

На цьому етапі важливо задокументувати докази, де вони зберігаються та в якому форматі вони зберігаються. Це може бути електронний лист або відеокліп, який вказує на подію, що розслідується.

Крок 3: Збір доказів

Етап збору цифрової криміналістики передбачає ретельне вилучення цих доказів, гарантуючи відсутність шкоди. Іноді цей крок такий же простий, як зробити копію жорсткого диска і прочесати її.

Однак це може бути не так просто, як здається у всіх сценаріях. Цей крок також може включати відновлення видалених файлів або злом паролів для отримання доступу.

На цьому етапі дані також вивчаються і при необхідності уточняються. Коли копиця сіна менше, голку легше знайти. Як тільки дані стають доступними, вони мають бути ізольовані та захищені від зміни. Створюються резервні копії, які гарантують, що весь вміст і метадані однакові.

Крок 4: Збереження доказів

Вихідні дані, які виступають в якості цифрових доказів, тепер ізольовані і не можуть бути оброблені ніким без повноважень. Криміналістичні зображення є точними копіями цифрових доказів, виконаних на бітовому рівні (0 або 1). Процес генерації цього образу бітового потоку називається створенням образу.

Хешування - це математичний алгоритм, який обробляє вихідний бітовий потік і зображення. Функція хешування створює унікальне значення для кожного унікального бітового потоку, який вона обробляє. Ці хеші розглядаються як «відбитки пальців» цифрових доказів. Образ та оригінальний цифровий доказ вважаються однаковими, якщо їхні відбитки пальців збігаються.

На цьому етапі встановлюється та документується процес розслідування (англ. Chain of custody). Цей документ має вирішальне значення, особливо якщо ці докази будуть використані в суді. Це детальний звіт про цифрові докази, починаючи з моменту, коли вони були отримані, і закінчуючи тим, коли вони були представлені в суді або аудиторській групі. Кожного разу, коли доказ переходить з рук в руки, він зазначається поруч з описом цього доказу в цей момент часу.

Крок 5: Аналіз інформації

На цьому етапі досліджуються всі відповідні цифрові дані, аналізуються та витягуються найбільш релевантні частини. Ця релевантна інформація конвертується у формат, який можна використовувати для представлення зацікавленим сторонам або суду.

Кількість часу, витраченого на цей етап, залежить від фактів події. У деяких випадках він може розтягнутися на тривалий період. Тут важливо пам'ятати про обставини та факти розслідування.

На етапі аналізу слідчі намагаються встановити часові рамки, виявити зв'язки, знайти незаконний контент, такий як дитяча порнографія, і визначити, чи стала система жертвою шкідливого програмного забезпечення або будь-якої іншої форми кібератаки.

До кінця цього етапу слідчі формують висновки. Прикладом може бути позначення «ймовірно» на запитання на кшталт «Чи був цей USB-накопичувач підроблений?».

Цей крок може зайняти багато ітерацій, щоб досягти бажаної точки закриття. Кожна дія на цьому етапі документується в інтересах повторюваності. Повторюваність необхідна для того, щоб уповноважена третя сторона могла дійти тих самих висновків, виконуючи ті самі кроки з тими самими інструментами щодо одного й того ж доказу. Це встановлює достовірність розслідування.

Крок 6: Презентація звіту

Документування - це крок, який проходить паралельно з кожним етапом процесу цифрової криміналістики. Після завершення розслідування всі висновки

охоплює документ після розслідування. Формат цього документа повинен відповідати вимогам суду або клієнта.

Більшість криміналістичних інструментів також автоматично генерують свої звіти для використання експертами. Вони є технічними і не можуть бути зрозумілі всім.

Тут на допомогу приходить презентаційна частина. Представлення цих доповідей залежить від цільової аудиторії. Наприклад, у суді презентація має бути достатньо простою, щоб суддя та присяжні могли її зрозуміти, висвітлюючи кроки, вжиті для отримання доказів. Презентація може зробити або зруйнувати справу на чиюсь користь.

Після інциденту, пов'язаного з кіберзлочинністю, більш технічно детальний звіт робить свою справу в технічному налаштуванні. Цей звіт стане відправною точкою для виправлення та можливих змін в інфраструктурі.

Виконуючи всі ці кроки, команда дослідників цифрової криміналістики гарантує, що:

- Жодні дані не втрачаються, не змінюються та не пропущені
- Вся аналізована інформація еквівалентна вихідним даним
- Здійснюється документування кожної людини, інструменту та дії
- Встановлено хронологію подій, що трапилися. [6]

1.5.3. Методи цифрової криміналістики

У комп'ютерно-криміналістичному розслідуванні використовуються різні методи, такі як:

1. Cross-drive analysis (CDA) - англ. перехресний аналіз - це техніка, яка дозволяє досліднику швидко ідентифікувати та співвіднести інформацію з кількох джерел даних або інформацію на кількох дисках. Існуючі підходи включають кореляцію з кількома дисками за допомогою текстового пошуку, наприклад, адрес електронної пошти, номер соціального страхування або номерів кредитних карток.

2. Живий аналіз. Він використовується для вивчення комп'ютерів всередині ОС за допомогою різних інструментів системного адміністрування та криміналістики, щоб отримати інформацію з пристрою. У криміналістичному

аналізі збір летючих даних дуже важливий, як встановлені програмні пакети, апаратна інформація і т.д. Цей підхід корисний у випадку, коли слідчий має справу з зашифрованими файлами. Якщо пристрій все ще активний і працює, коли він передається досліднику, дослідник повинен зібрати всю нестабільну інформацію з пристрою, таку як історія входу користувача, які порти TCP і UDP відкриті, які служби в даний час використовуються, і запущені і т.д.

3. Відновлення видалених файлів: це техніка, яка використовується для відновлення видалених файлів. Видалені дані можуть бути відновлені або жадані за допомогою судових інструментів, таких як CrashPlan, OnTrack EasyRecovery, Wise Data Recovery тощо.

4. Стеганографія - це техніка приховування секретної інформації всередині або поверх чогось, що щось може бути чим завгодно від зображення до будь-якого типу файлу. Комп'ютерні криміналісти можуть протистояти цьому, переглядаючи та порівнюючи хеш-значення зміненого файлу та оригінального файлу, хеш-значення буде різним для обох файлів, навіть якщо вони можуть виглядати ідентичними при візуальному огляді. [7]

1.6. Висновок. Постанова задачі.

Таким чином, проаналізувавши наявну інформацію про галузь цифрової криміналістики, процедура розслідування інциденту може здатися складною і надлишковою, проте щоб обґрунтувати протилежне за мету було поставлено - дослідити наявні методи цифрової криміналістики і обрати найоптимальніші для розслідування змодельованого інциденту. З допомогою обраних методів зібрати доказову базу, описати картину того, що сталося і запропонувати план дій щодо усунення наслідків інциденту..

Для досягнення поставленої мети було виконано наступні завдання:

1. Обрано одну з найпоширеніших типів вразливостей;
2. В тестовому середовищі розгорнуто завідома вразливий сервіс;
3. Змодельована поведінка злочинця шляхом експлуатації вразливості;
4. Проведено розслідування змодельованого інциденту;
5. Створено план, щодо усунення наслідків інсценованого інциденту.

2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1.Модель порушника

Запобігти реальним та потенційним загрозам у комп'ютерній системі, забезпечити надійний захист інформації можливо лише за умов визначення усіх реальних та потенційних категорій порушників, а також методів, які вони використовують.

Порушником вважається особа, що випадково або усвідомлено з корисливих інтересів або без такого (наприклад, з метою самоствердження) здійснила спробу виконання заборонених у автоматизованій системі дій, використовуючи для цього різні методи та засоби.

Зловмисником, називають порушника, що навмисно йде на порушення з корисливих спонукань.

Для визначення плану дій щодо захисту інформації в автоматизованій системі у кожній конкретній ситуації, виходячи з визначеної технологи обробки інформації, має бути визначена модель порушника, яка повинна адекватно відображати його можливості щодо втручання у роботу системи.

Неформальна модель порушника за суттю є описом його реальних або теоретичних можливостей, апріорних знань, технічної оснащеності, часу та місця дії тощо. Слід враховувати, що для досягнення своїх цілей порушник повинен прикласти деякі зусилля, затратити певні ресурси. Детально дослідивши умови порушень, у деяких випадках можна або вплинути на причини їх виникнення з метою їх усунення, або точніше визначити вимоги до системи захисту від даного виду порушень або злочинів.

Під час розробки моделі порушника встановлюються:

- припущення щодо категорії осіб, до яких він належить;
- припущення щодо мотивів та мети його дій;
- припущення щодо його кваліфікації та технічної оснащеності, застосованих методів та засобів;
- обмеження й припущення про характер можливих дій.

По відношенню до інформаційних ресурсів розрізнять категорії внутрішніх порушників (персонал підприємства) або зовнішніх порушників (сторонні особи). Внутрішнім порушником може бути особа з наступних категорій персоналу, що має доступ у будинки й приміщення, де розташовані компоненти автоматизованої системи:

– користувачі (оператори) автоматизованої системи;

– персонал, що обслуговує технічні засоби системи: інженери, техніки;

– співробітники відділів розробки й супроводження програмного забезпечення: системні та прикладні програмісти;

– технічний персонал, якій обслуговує будівлі: сантехніки, електрики, прибиральники тощо;

– співробітники служби охорони;

– керівники різних рівнів посадової ієрархії.

До сторонніх осіб, що можуть бути порушниками, слід віднести наступні категорії осіб:

– партнери підприємства або його клієнти - фізичні або юридичні особи;

– відвідувачі, що звернулися з власних справ або запрошені з будь-якого питання;

– співробітники підприємств постачальників товарів та послуг, включаючи забезпечення життєдіяльності об’єкту інформаційної діяльності (зв'язок, ліфтове господарство, утримання систем сигналізації та відео спостереження, енерго-, водо-, теплопостачання тощо);

– співробітники підприємств - конкурентів, іноземні делегації;

– особи, випадково або навмисне порушили режим доступу на об’єкт інформаційної діяльності;

– співробітники дипломатичний місій або спецслужб. Останні можуть видавати себе за будь-яку категорію з тих, що перелічені вище;

– будь-які особи за межами контрольованої території.

Можна виділити три основні мотиви порушень: недбалість (безвідповідальність), самоствердження (помста) і корисливий інтерес.

У випадку порушень, що обумовлені безвідповідальністю, користувач цілеспрямовано або випадково провадить які-небудь руйнуючі дії, не зв'язані проте зі злим наміром. У більшості випадків це слідство некомпетентності або недбалості.

Деякі користувачі вважають одержання доступу до системних наборів даних великим успіхом, затіваючи свого роду гру «користувач - проти системи» заради самоствердження або у власних очах, або в очах колег.

Порушення безпеки інформаційної системи може бути викликане й корисливим інтересом користувача системи. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для доступу до збереженої, переданої й оброблюваної у системі інформації.

Порушників можна класифікувати наступним чином:

За рівнем знань про інформаційну систему:

– знає функціональні особливості системи, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

– має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговування;

– має високий рівень знань в області програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

– знає структуру, функції й механізм дії засобів захисту, їх сильні й слабкі сторони.

За рівнем можливостей та використовуваним методам і засобам:

– застосовує чисто агентурні методи здобування відомостей або втручання у роботу автоматизованої системи;

– застосовує нештатні пасивні методи та технічні засоби перехоплення інформації без модифікації компонентів системи;

– використовує тільки штатні засоби й недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесені через пости охорони;

– застосовує методи й засоби активного впливу на інформаційні ресурси, їх модифікації шляхом застосування спеціальних апаратно-програмних засобів, технічних приладів, які підключені до каналів передачі даних, впровадження програмних закладок, використання спеціального програмного забезпечення.

За часом дії:

– у процесі функціонування автоматизованої системи або її окремих компонентів;

– у період не активності компонентів системи, поза робочим часом, під час планових перерв у її роботі для обслуговування та ремонту тощо;

– як у процесі функціонування системи, так і в період не активності її компонентів.

За місцем дії:

– без доступу на контрольовану територію;

– з контрольованої території без доступу в будівлі та споруди;

– усередині приміщень, але без доступу до технічних засобів системи;

– з робочих місць кінцевих користувачів або операторів;

– з доступом у зону сховищ даних (ресурси, що знаходяться у статусі хостингу, бази даних, архіви тощо);

– з доступом у зону керування засобами забезпечення безпеки.

Доцільно враховувати наступні обмеження й припущення про характер дій можливих порушників:

– порушник, плануючи спроби несанкціонованих дій, може приховувати їх від інших співробітників;

– робота з добору кадрів і спеціальні заходи ускладнюють спроби створення коаліцій двох і більш порушників, тобто їх змови та узгоджених дій з метою подолання підсистеми захисту;

– несанкціоновані дії можуть бути наслідком прорахунків у системі навчання та підготовки персоналу, помилок користувачів та адміністраторів автоматизованої системи, а також недоліків прийнятої технології обробки інформації.

Слід зауважити, що визначення конкретних значень характеристик потенційних порушників у значній мірі суб'єктивно, тому доцільно створювати модель порушника групою досвідчених експертів.

В цілому, модель порушника, що побудована з урахуванням особливостей конкретної предметної області й технології обробки інформації, може бути представлена перерахуванням декількох варіантів його виду. Кожний вид порушника повинен бути охарактеризований значеннями характеристик, наведених вище.

Зокрема, нормативні документи системи криптографічного захисту інформації (КЗІ), залежно від вірогідних розумів експлуатації засобів криптографічного захисту інформації та відповідно до цінності інформації, що захищається, визначаються чотири рівні можливостей порушника:

нульовий рівень - ненавмисне порушення конфіденційності, цілісності та підтвердження авторства інформації;

перший рівень - порушник має обмежені засоби та самостійно створює засоби, розробляє методи атак на засоби КЗІ, а також інформаційно-телекомунікаційні системи із застосуванням широко розповсюджених програмних засобів та електронно-обчислювальної техніки. Саме до цього рівня може належати потенційний порушник в моделі, що розглядатиметься далі;

другий рівень - порушник корпоративного типу має змогу створення спеціальних технічних засобів, вартість яких співвідноситься з можливими фінансовими збитками, що виникатимуть від порушення конфіденційності, цілісності та підтвердження авторства інформації, зокрема при втраті, спотворенні

та знищенні інформації, що захищається. У цьому разі для розподілу обчислень при проведенні атак можуть застосовуватися локальні обчислювальні мережі;

третій рівень - порушник має науково-технічний ресурс, який прирівнюється до науково-технічного ресурсу спеціальної служби економічно розвиненої держави.

Слід звернути увагу, у силу непередбачуваності усіх можливостей порушника, навіть якщо у автоматизованій системі створюється комплекс засобів захисту, що роблять таке проникнення надзвичайно складним, повністю захистити її від проникнення «на всі 100%» практично неможливо.[8]

2.2. Алгоритм інциденту

В роботі розглядається модель із двох хостів - зловмисник і жертва. Потенційно вони знаходяться в одній мережі, оскільки зловмисник має можливість мережевої взаємодії із жертвою. Подібна доступність може бути забезпечена не тільки подібним сценарієм, але задля спрощення було використано саме її.

За рахунок подібного рівня доступності порушник має можливість поверхневого аналізу захищеності цілі, тобто провести найперший етап будь-якої атаки - розвідки. Для ідентифікації цілі як правило використовуються різного роду сканери, наприклад, masscan, nmap, nikto та їм подібні.

Після визначення сервісів, які працюють на хості-жертві порушник намагається визначити, які з них мають вразливості і, в залежності від результатів, експлуатує їх або шукає нову ціль.

Моделювання інциденту проходитиме за наступним алгоритмом:

1. Створення контейнерів:

– Необхідно створити два Docker-контейнери - один атакуючий, інший для жертви.

– Забезпечити належні мережеві налаштування для взаємодії контейнерів.

2. Налаштування SSH-сервера:

– Встановити та налаштувати SSH-сервер на контейнері-жертві.

– Зробити внутрішні налаштування SSH для спрощення атаки (наприклад, слабкий пароль, велика тривалість блокування після помилкових спроб).

– Ввімкнути системи моніторингу та журналювання, щоб відстежувати незвичайну активність.

3. Брутфорс SSH на контейнері "атакуючий":

– Встановити один з доступних в репозиторії інструмент для брутфорс атак.

– Використати інструмент для брутфорсу, такий як Hydra або Medusa, для запуску атаки на SSH-сервер контейнера "жертва".

– Ввести список можливих імен користувачів та паролів для спроб атаки.

– Аналіз результатів і спостереження за можливими вразливостями.

4. Моніторинг та журналювання:

– Аналіз логів для виявлення спроб брутфорсу та інших можливих загроз.

5. Вдосконалення заходів безпеки:

– Виправлення виявлених вразливостей та вдосконалення заходів безпеки на контейнері-жертві.

– Розглянути можливість використання інструментів для виявлення та захисту від атак на проникнення, таких як файрволи, системи виявлення вторгнень та інші.

2.3.Моделювання інциденту

В якості інциденту було обрано атаку на паролі методом перебору, відому також як атаку грубою силою або brute force attack. За рейтингом OWASP TOP 10 з другої позиції в рейтингу 2017-го року цей тип атак перемістився на 7-му позицію в останньому актуальному рейтингу - 2021-го року (Рисунок 2.1). Також він був перейменований з Broken Authentication у Identification and Authentication Failures.[9] Проте, зміна позиції у рейтингу не робить цей тип атак менш небезпечним або руйнівним через постійно зростаючу кількість комбінацій логінів та паролів, які регулярно зливають до мережі.

Brute force - це тип кібератаки, який ґрунтується на методі проб і помилок: зловмисник надсилає безліч паролів, доки не вгадає правильну комбінацію символів і не отримує доступ до облікового запису довіреного користувача. Такі атаки неймовірно поширені з двох причин:

– їх легко виконати за допомогою безкоштовних інструментів, сценаріїв автоматизації та баз даних паролів

– Багато користувачів покладаються на слабкі паролі, які вгадуються за лічені секунди. [10]

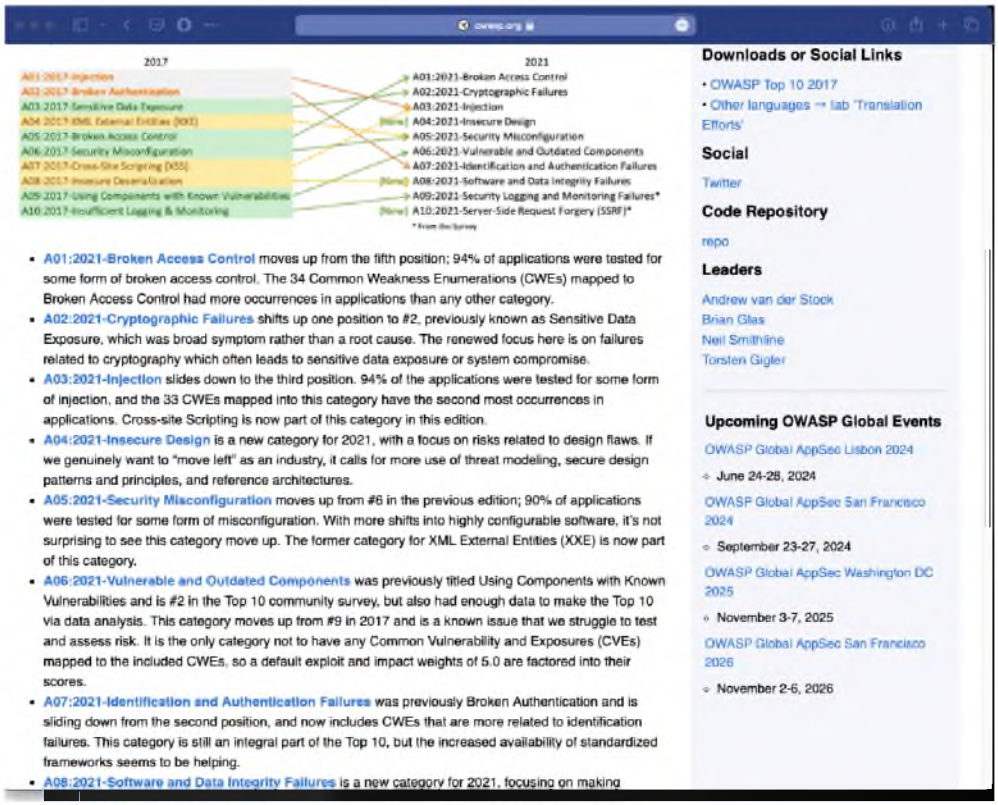

Рисунок 2.1 - Рейтинг OWASP TOP 10 порівняння 2021-го та 2017-го років

Для моделювання інциденту знадобиться 2 ОС - нападник і жертва. В якості постраждалої системи було обрано Debian 12, а для симуляції атаки проводитиметься з kali linux 2023.3. Обидві системи розгорнуті у вигляді контейнерів в Docker під архітектуру ARM. Процес розгортання контейнерів зображено на рисунках 2.2 - 2.5. Інформація про системи наведено на рисунках 2.6 і 2.7.

Docker - це інструмент, який використовується для автоматизації розгортання додатків у легких контейнерах, щоб програми могли ефективно працювати в різних середовищах ізольовано. Це набір продуктів «платформа як послуга» (англ. PaaS), які використовують віртуалізацію на рівні ОС для доставки програмного

забезпечення в пакетах, які називаються контейнерами. Програмне забезпечення, на якому розміщуються контейнери, називається Docker Engine. Вперше він був випущений у 2013 році та розроблений компанією Docker, Inc. [11]

```
oleksandrtsyhanov@Oleksandrs-MacBook-Air ~ % docker run -it --privileged debian /bin/bash
root@0b63b0d65ba7:/#
```

Рисунок 2.2 - Розгортання контейнеру з Debian 12

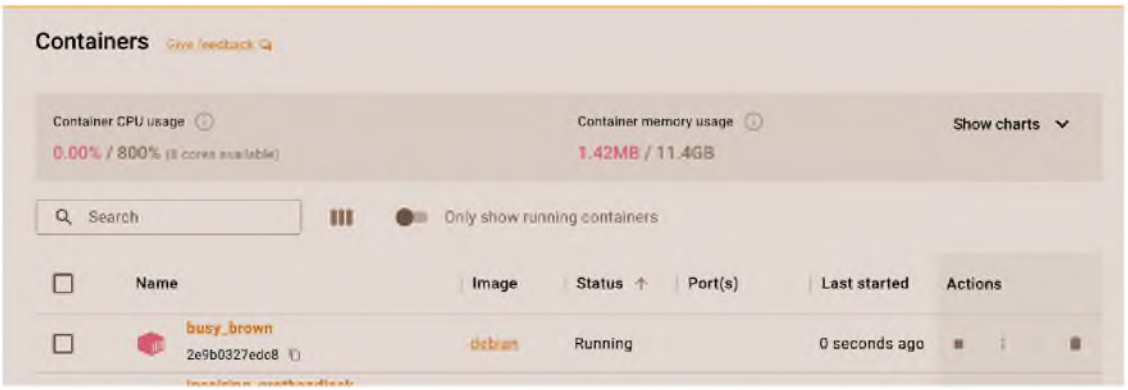

Рисунок 2.3 - Запущений контейнер з Debian в графічному інструменті Docker desktop

```
oleksandrtsyhanov@Oleksandrs-MacBook-Air ~ % docker run -it --privileged kalilinux/kali-rolling /bin/bash
┌──(root㉿0c4569d3ab84)-[/]
└─#
```

Рисунок 2.4 - Розгортання контейнеру з Kali linux 2023.3

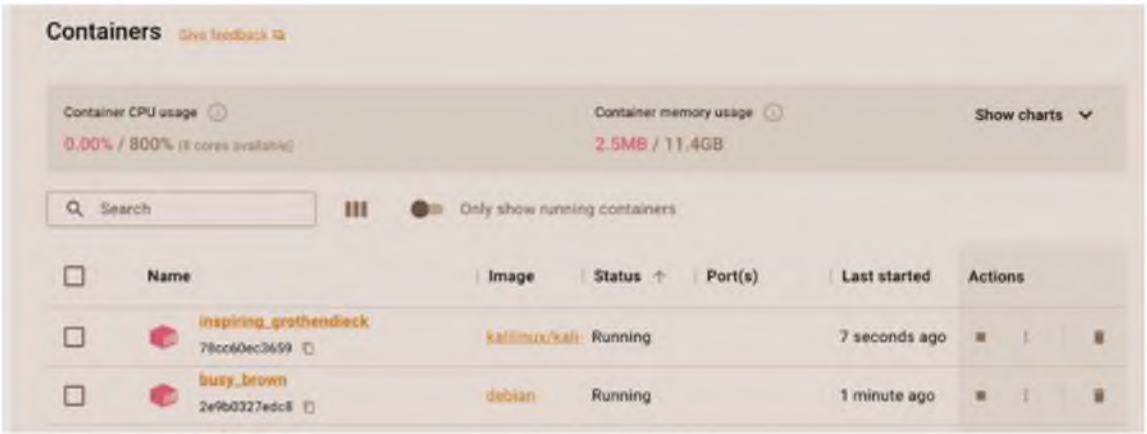

Рисунок 2.5 - Запущений контейнер з Kali linux в графічному інструменті Docker desktop

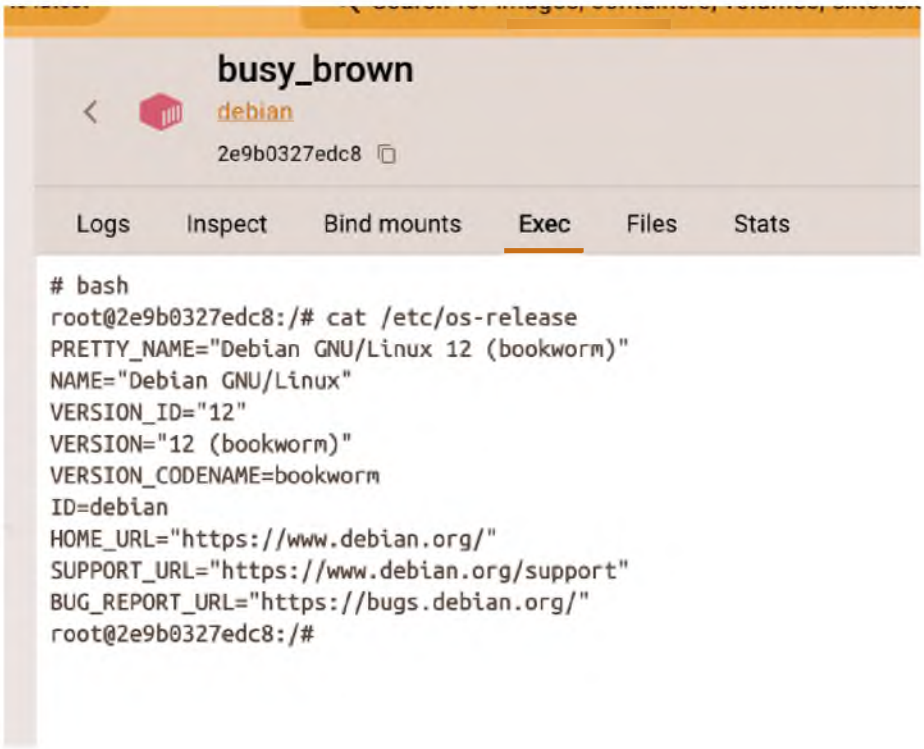

Рисунок 2.6 - Контейнер-жертва під управлінням Debian 12

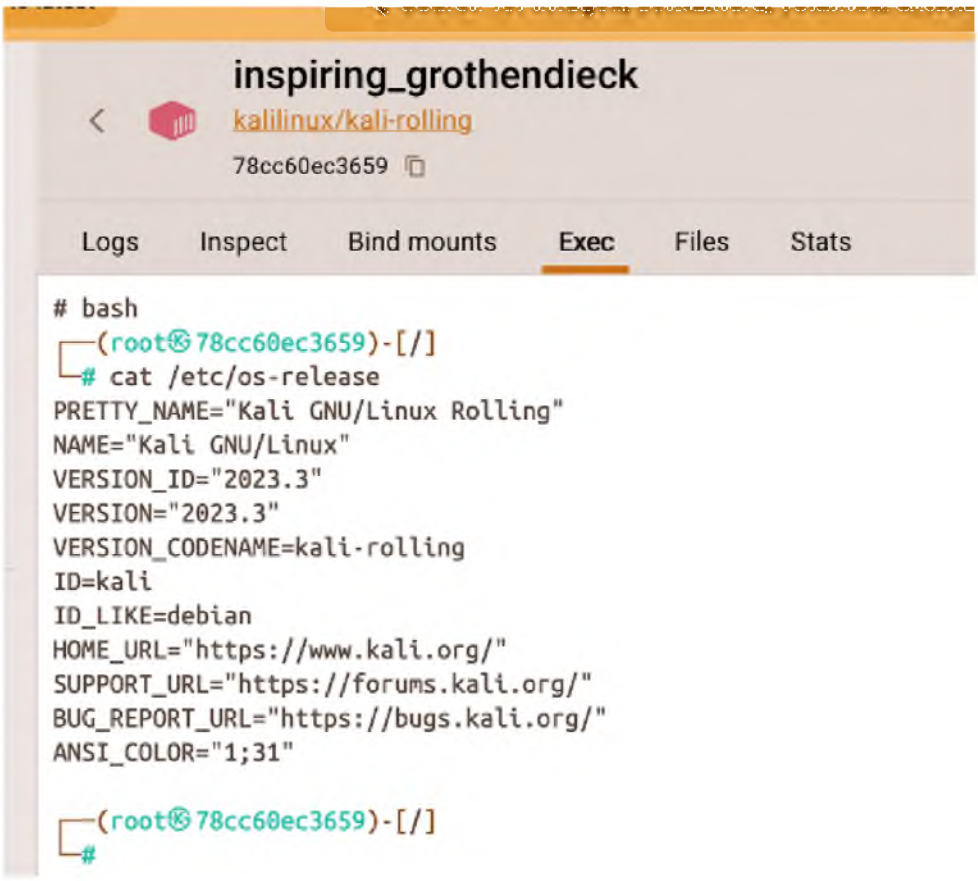

Рисунок 2.7 - Контейнер-нападник під управлінням Kali linux 2023.3

Усі linux контейнери за замовчуванням запускаються з привілейованими користувачами (root). Підбір паролю виконувався до сервісу SSH, який є основним інструментом для віддаленої роботи з комп'ютерами під управлінням ОС на основі unix. Щоб не займатися додатковою конфігурацією SSH, було створено непривілейованого користувача.

Рисунок 2.8 - Створення користувача test_user і зміна паролю до нього

Щоб впевнитися, що все налаштовано вірно, зроблена спроба підключення меж контейнерами через SSH.

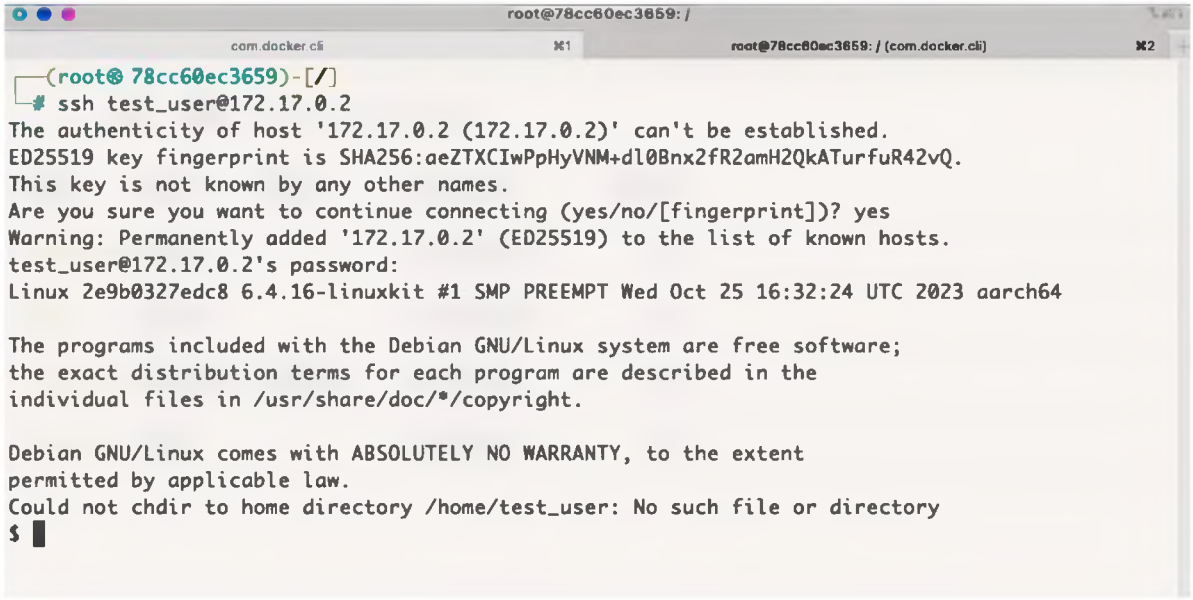

Рисунок 2.9 - Підключення по SSH з Kali linux на Debian

Оскільки умовний порушник для перебору паролів використовував би словник з паролями, було взято перший, який вдалося знайти у відкритому доступі на Github.

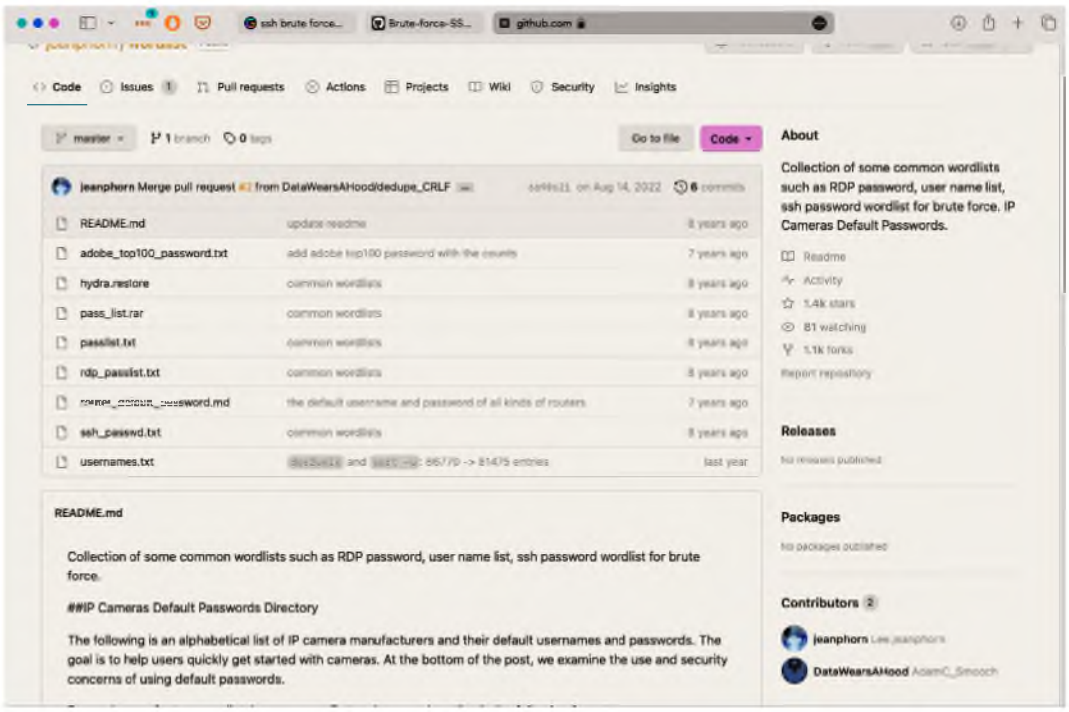

Рисунок 2.10 - Репозиторій на Github зі словникам паролів

Цей список треба завантажити до системи, з якої проводитиметься атака.

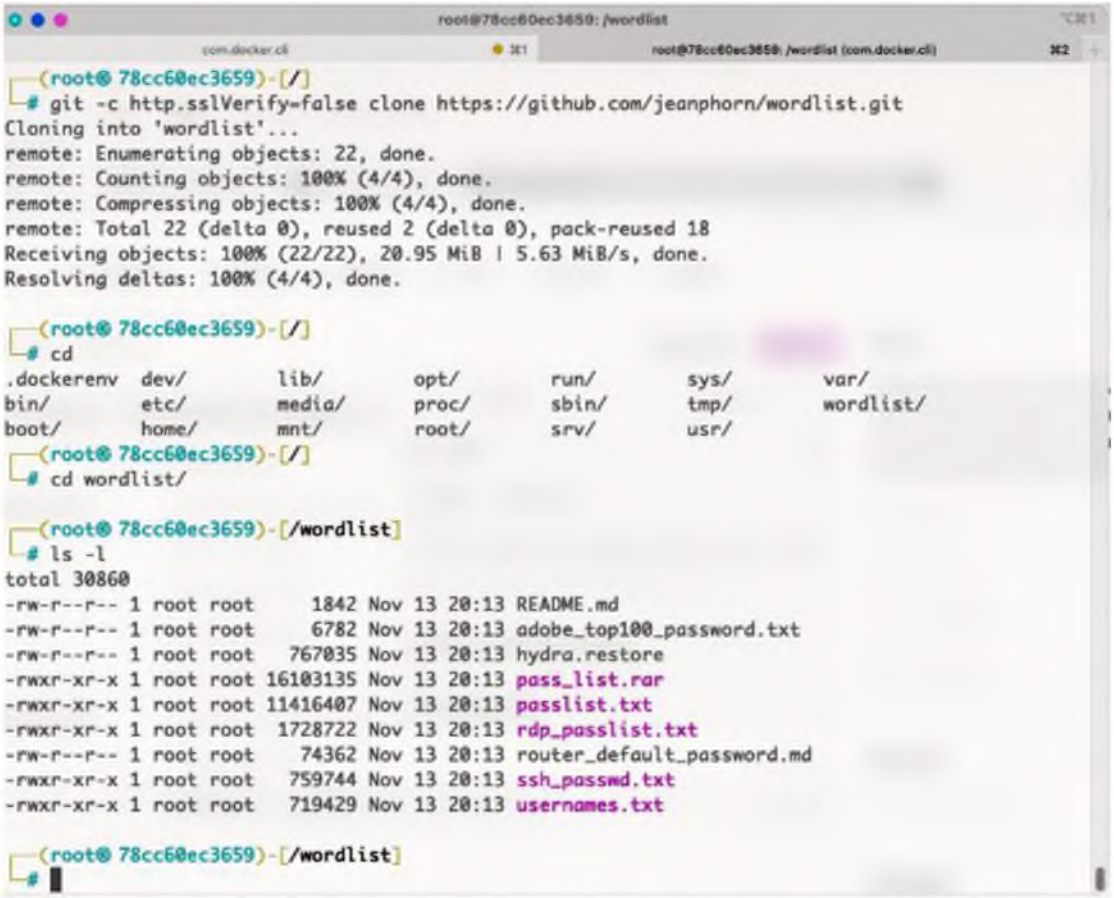

Рисунок 2.11 - Процес завантаження словника

Для перебору паролів існує безліч різних інструментів з різним функціоналом, від відносно простого nmap, який має скрипти для перебору паролів, до більш функціональної hydra та Burp Suite.

Для симуляції було обрано hydra - це інструмент для зламу авторизації, здатний працювати в багатопоточному режимі і який підтримує численні протоколи для атак. Він дуже швидкий і гнучкий, а нові модулі легко додавати. Цей інструмент дозволяє дослідникам і консультантам з безпеки показати, як легко отримати несанкціонований доступ до системи віддалено.[12]

Щоб запустити підбір паролю до SSH достатньо виконати команду: hydra -l test_user -P SSH_passwd.txt 172.17.0.2 SSH, де

l - ім'я користувача;

P - файл-словник з паролями

SSH_passwd.txt - назва файлу з паролями (використувується в якості значення параметру -P);

172.17.0.2 - IP адреса контейнера-цілі

SSH - сервіс, до якого підбирається пароль (працює лише за умови, коли сервіс використовує стандартний порт для роботи, в іншому випадку необхідно вручну вказувати порт, на якому працює цільовий сервіс).

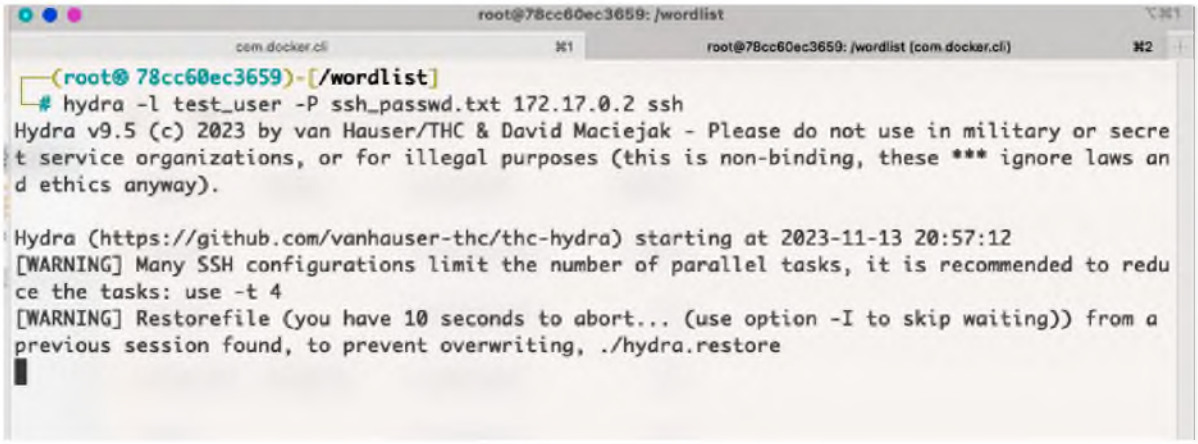

Рисунок 2.12 - Процес роботи hydra

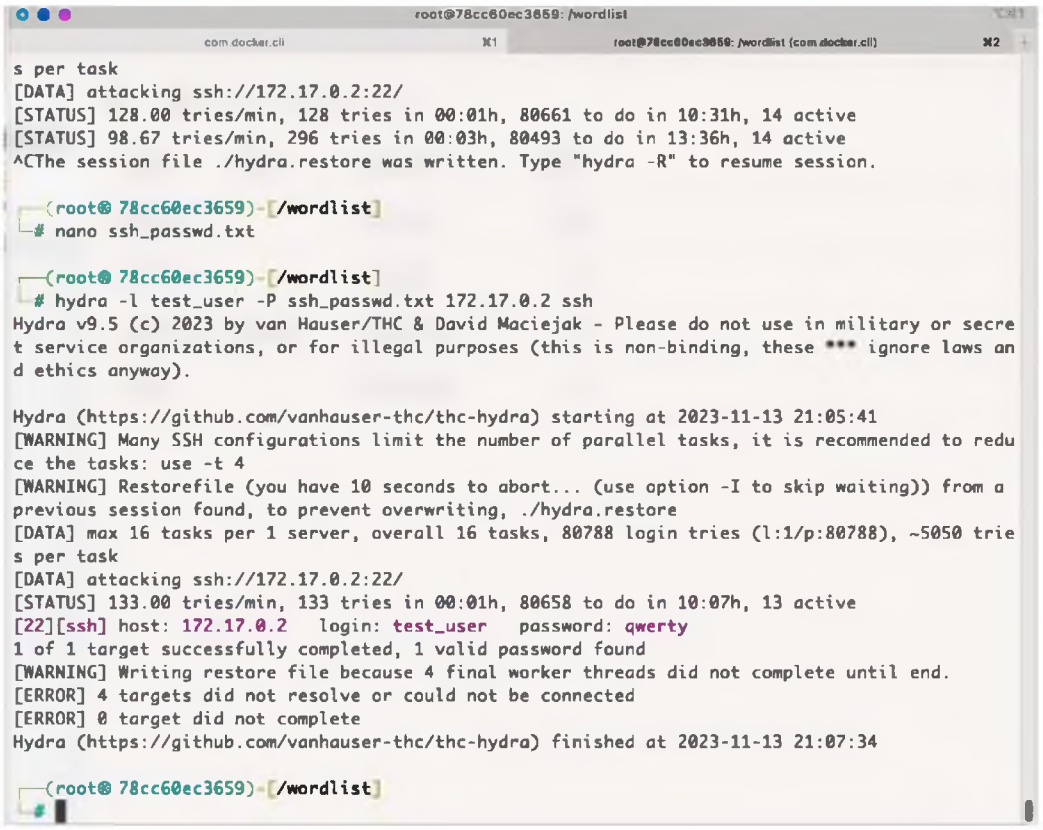

Рисунок 2.13 - Результати роботи hydra

Тепер можна спробувати під’єднатися до цільової ВМ з отриманими даними авторизації.

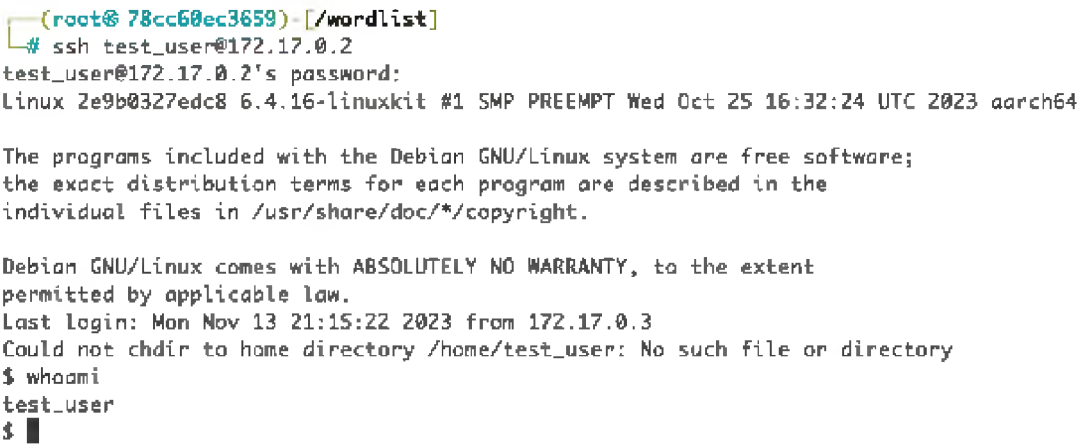

Рисунок 2.14 - Успішна авторизація з даними test_user-а

На цьому моделювання інциденту завершено. Зловмисник отримав доступ до цільового хоста.

2.4.Методи виявлення інциденту

Існує безліч методів для виявлення інцидентів, але у всіх є одна спільна частина - щоб ці засоби були ефективними, їм потрібен або механізм автоматичного сповіщення про підозрілу активність, або певна кількість людей для постійного моніторингу показників. Виявити інциденти можуть допомогти наступні засоби:

1. Системи виявлення вторгнень (IDS) - використовуються для автоматичного виявлення аномальної або зловмисної активності.
2. Мережевий моніторинг - моніторинг трафіку за допомогою інструментів, таких як Wireshark або Snort, для виявлення незвичайних закономірностей та підозрілої активності.
3. Аналіз журналів - для ефективного моніторингу та аналізу слід використовувати інструменти аналізу журналів, такі як ELK Stack або Splunk
4. Моніторинг заходів безпеки - системи моніторингу інцидентів безпеки для виявлення змін у конфігураціях, спроб входу та інших подій, що можуть свідчити про інцидент.
5. Системи аналізу вразливостей - використовуються для виявлення слабких місць у системі, які можуть бути використані для атак.

Окремо можна виділити SIEM та SOAR системи. SIEM (security information and event management) здатна збирати, аналізувати та оброблювати дані з файлів журналів безлічі різних систем під управлінням різних операційних систем, а також вони можуть генерувати повідомлення про інциденти безпеки і надсилати їх до будь-якого зручного місця - від месенджерів до електронної пошти. SOAR системи також дозволяють налаштувати засоби протидії інцидентам в залежності від потреб організації.

2.5. Застосування методів цифрової криміналістики

При реагуванні на інциденти пов’язані з атакою на паролі можна виділити декілька питань, на які необхідно отримати відповідь по завершенню розслідування:

1. Яка з існуючих на підприємстві систем була атакована?

2. До облікового запису якого користувача порушник намагався отримати доступ?

3. Чи була активність легітимною або це була атака з метою отримання неправомірної вигоди?

4. Встановлення причетної особи за можливості.

Як вже згадувалось раніше, встановлення причетних до атаки може бути досить складною задачею, оскільки зловмисники можуть використовувати різні засоби для маскування як своєї особистості, так і свого місцезнаходження, що значно ускладнює пошук причетних, а також значно підвищує вартість розслідування. В цьому випадку необхідно зберегти баланс, щоб витрати на розслідування не перевищували вартості ризику.

При розслідуванні інциденту зі спробою перебору паролів використовуються наступні методи цифрової криміналістики:

1. Збір доказів: клонування даних. В загальному випадку, виконується клонування всього диску з атакованої системи. Це може знадобитися, якщо зловмисник не обмежився зламом доступу, або йому вдалося отримати привілейований доступ до системи і встановити на ній шкідливе ПЗ. В таких випадках не вдасться обмежитися копією файлів журналів

2. Аналіз даних (комп'ютерна форензика) - Аналіз жорстких дисків, файлових систем, реєстраційних записів та інших цифрових слідів. Рішення про необхідність аналізу диску приймається лише після встановлення факту зараження атакованої системи шкідливим ПЗ, в інших випадках варто обмежитися аналізом файлів журналів для отримання більш детальної інформації про події інциденту.

Для клонування даних існує безліч інструментів в залежності від середовища, де ці дані зберігалися. Якщо мова про енергонезалежні накопичувачі (жорсткі диски або SSD накопичувачі), то для їх клонування можуть використовуватися програмні засоби, наприклад інструмент unix систем такий як dd. Для віртуального середовища, для управління яким використовується гіпервізор, можна використовувати як повну копію враженої системи так і систему снапшотів, які можуть бути як досить швидко збережені, так і швидко розгорнуті. При

використанні снапшотів є можливість зберегти зміст оперативної пам'яті, що робить зручним використання даного інструменту.

2.6.Заходи щодо розслідування інциденту

Найпершим етапом розслідування будь-якого інциденту буде його виявлення. Способів для цього може бути безліч, від профілактичної перевірки логів авторизації, до спрацювання систем виявлення вторгнень (англ. IDS - intrusion detection system). Найгірший випадок, як можна виявити подібний інцидент, це коли зловмиснику вдалося підібрати дані для авторизації і порушити цілісність або конфіденційність даних, змінивши їх або викравши відповідно.

В роботі не використовувалися IDS або SIEM системи, але нехай обрано не найгірший сценарій і до виявлення інциденту призвело блокування важливого облікового запису, що в деякій мірі порушує роботу сервісу, який розгорнутий на хосту. Тобто ігнорувати або не помітити проблему досить важко.

На другому етапі необхідно ізолювати систему від будь-якого впливу. Якщо це віртуальне середовище, фізичний ПК або сервер, достатньо буде ізолювати на мережевому рівні, оскільки зловмиснику для очищення логів від своєї присутності потрібен буде фізичний доступ до дисків, що частіше за все, неможливо, якщо це не хтось зі співробітників. На прикладі docker контейнера ізоляцію від середовища можна виконати шляхом відключення його від загальної мережі, як на рисунку 2.15. Команда docker network має 3 аргументи (по порядку): операція (connect/disconnect), id мережі, id контейнера. В інших типах інцидентів ізоляція постраждалого пристрою може включати в себе зберігання у клітці Фарадея та забезпечення йому належного рівня захисту (наприклад, окрема кімната з електронним замком з авторизацією за біометричними даними, тощо).

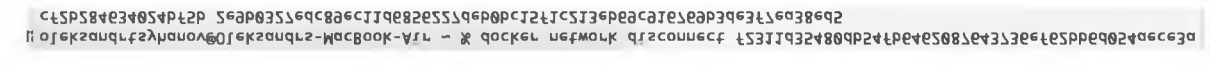

Рисунок 2.15 - Виключення контейра з атакованої мережі

Тобто якщо зараз спробувати підключитися до контейнера і відобразити його налаштування мережі, то можна побачити лише локальний інтерфейс (т.з. loopback) з адресою 127.0.0.1. Етап з клонуванням атакованої системи було пропущено через

складність реалізації в середовищі, де проводилось моделювання, але при моделюванні на віртуальних машинах така можливість вже була б (рис. 2.16).

Рисунок 2.16 - Приклад можливості клонування віртуальної машини

Рисунок 2.17 - Ізольоване середовище, готове до проведення розслідування

Наступним етапом розслідування є безпосередньо збір та аналіз доказів. За ідеальних умов, необхідно створювати копію постраждалої системи. Якщо це фізичний накопичувач, то робити його побайтову копію утилітою накшталт dd. У випадку віртуального середовища, гіпервізор дозволяє створювати безмежну кількість копій віртуальних машин або знімків її стану (snapshots). Для розслідування атаки на пароль до SSH достатньо буде отримати файл логів /var/log/auth.log. Для того, щоб його скопіювати на локальний диск існує інструмент docker cp, синтаксис якого деякою мірою нагадує scp: docker cp <containerId>:/file/path/within/container /host/path/target. На цьому етапі хост можна вимикати, оскільки ніяких енергозалажних даних при розслідуванні даного інциденту отримати не вдастся. Хоча при більш складних атаках цілком вірогідно, що найпершим після ізоляції середовища необхідно буде отримати енергозалежні дані, а вже потім збирати файли логів і т.д.

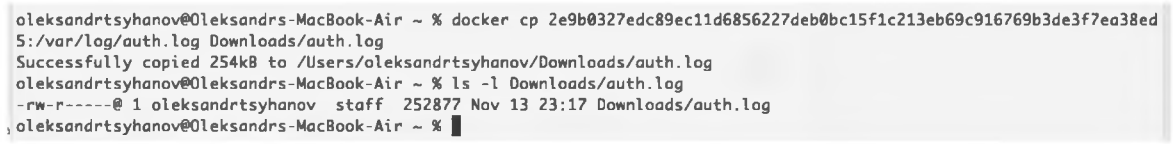

Рисунок 2.18 - Файл логів з контейнера успішно скопійовано на локальний накопичувач

Одним із найуніверсальніших інструментів для пошуку логів за ключовими словами є grep. Він дозволяє шукати співпадіння за найрізноманітнішими патернами - від збігів по ключовим комбінаціям символів, до регулярних виразів, які можуть бути унікальними для певних подій. Це значно зменшує вибірку даних, яку доведеться аналізувати спеціалісту.

Рисунок 2.19 Пошук співпадінь у файлі логів за ключовим словом

На рисунках 2.20 (а-б) зображені відривки файлу логів /var/log/auth.log, які є стандартним файлом журналів авторизації на Debian-based linux системах. В цих файлах логи 2-х сервісів - безпосередньо SSH та PAM (prioritized access management). Ці файли журналів мають наступну структуру:

1. Для SSH - yyyy-mm-dd:hh:mm:ss.%s%s%s%s%s%s <hostname>(у прикладі це ідентифікатор docker гонтейнера) ім’я_сервісу[id процесу]: <Повідомлення про невдалу спробу авторизації> for <ім’я користувача> from <ip адреса - джерело атаки> port <порт-джерело пакету>
2. Для PAM - yyyy-mm-dd:hh:mm:ss.%s%s%s%s%s%s <hostname>(у прикладі це ідентифікатор docker гонтейнера) ім’я_сервісу[id процесу]: <повідомлення>. Далі в залежності від повідомлення в довільному порядку можуть бути користувач, під яким зловмисник намагався увійти в систему, IP адреса і порт, з яких був трафік.

На цих відривках видно невдалі спроби авторизації і факт успішної авторизації після цього. Цих двох фактів вже достатньо, щоб класифікувати інцидент як brute-force атаку і те, що атака була успішною (на другому рисунку зображений факт успішної авторизації після перебору паролів). Оскільки файл логів зберігає в собі адресу та порт, з якого відправлялися невдалі спроби авторизації, це дозволяє спробувати відслідкувати, звідки виконувалася атака.

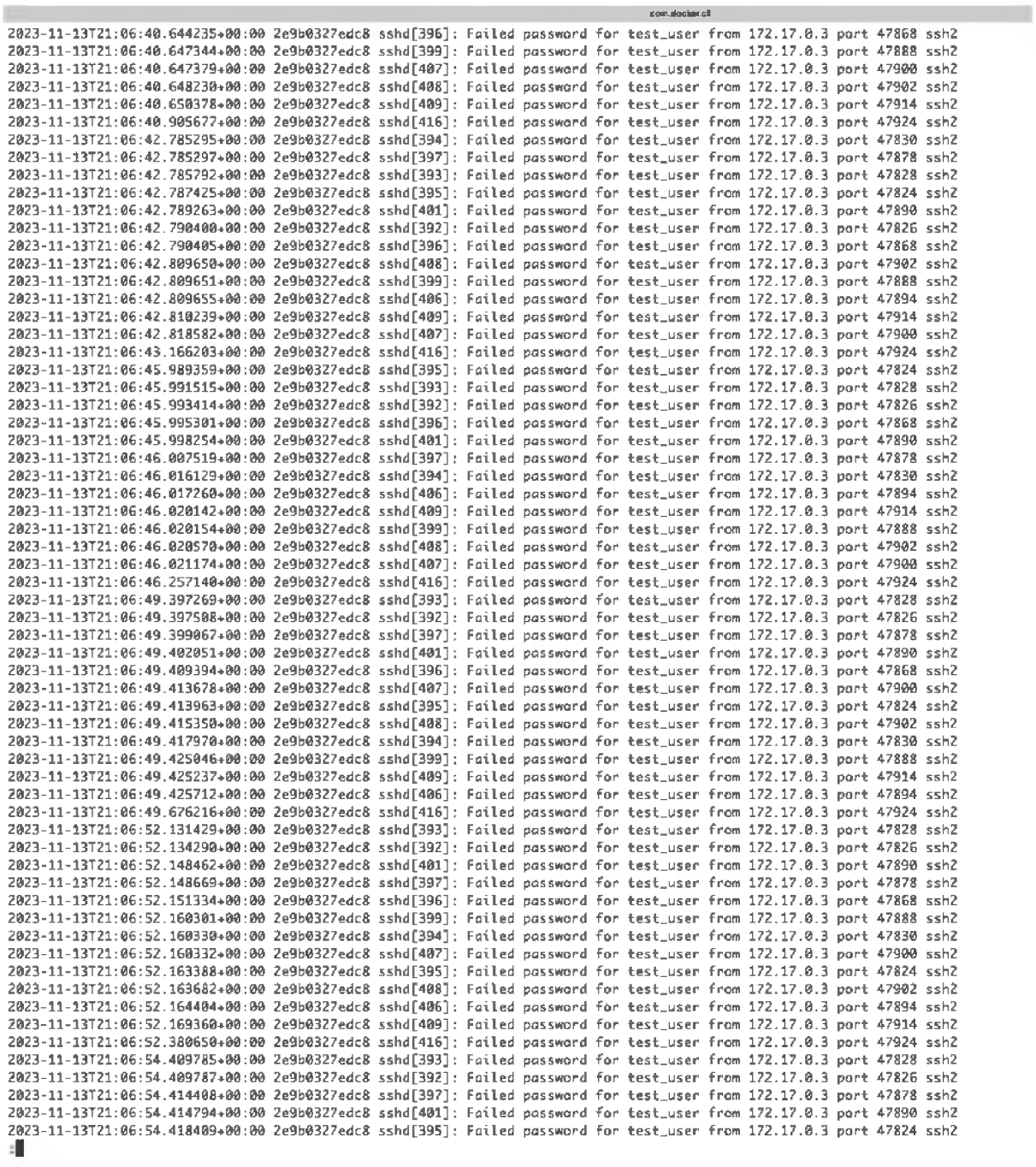

Рисунок 2.20 (а) - Масові невдалі спроби авторизації по SSH (сервісні логи)

```
com.docker.cli
2023-11-13T21:07:28.027539+00:00 2e9b0327edc8 sshd[442]: Failed password for test_user from 172.17.0.3 port 47696 ssh2
2023-11-13T21:07:29.660798+00:00 2e9b0327edc8 sshd[423]: Failed password for test_user from 172.17.0.3 port 47640 ssh2
2023-11-13T21:07:29.660799+00:00 2e9b0327edc8 sshd[421]: Failed password for test_user from 172.17.0.3 port 47624 ssh2
2023-11-13T21:07:29.660853+00:00 2e9b0327edc8 sshd[418]: Failed password for test_user from 172.17.0.3 port 47596 ssh2
2023-11-13T21:07:29.661743+00:00 2e9b0327edc8 sshd[422]: Failed password for test_user from 172.17.0.3 port 47626 ssh2
2023-11-13T21:07:29.664449+00:00 2e9b0327edc8 sshd[419]: Failed password for test_user from 172.17.0.3 port 47604 ssh2
2023-11-13T21:07:29.676534+00:00 2e9b0327edc8 sshd[426]: Failed password for test_user from 172.17.0.3 port 47650 ssh2
2023-11-13T21:07:29.678385+00:00 2e9b0327edc8 sshd[430]: Failed password for test_user from 172.17.0.3 port 47658 ssh2
2023-11-13T21:07:29.678412+00:00 2e9b0327edc8 sshd[420]: Failed password for test_user from 172.17.0.3 port 47614 ssh2
2023-11-13T21:07:29.678729+00:00 2e9b0327edc8 sshd[437]: Failed password for test_user from 172.17.0.3 port 47674 ssh2
2023-11-13T21:07:29.684650+00:00 2e9b0327edc8 sshd[427]: Failed password for test_user from 172.17.0.3 port 47652 ssh2
2023-11-13T21:07:29.686619+00:00 2e9b0327edc8 sshd[431]: Failed password for test_user from 172.17.0.3 port 47660 ssh2
2023-11-13T21:07:29.688592+00:00 2e9b0327edc8 sshd[434]: Failed password for test_user from 172.17.0.3 port 47656 ssh2
2023-11-13T21:07:29.965922+00:00 2e9b0327edc8 sshd[442]: Failed password for test_user from 172.17.0.3 port 47696 ssh2
2023-11-13T21:07:31.243543+00:00 2e9b0327edc8 sshd[430]: Accepted password for test_user from 172.17.0.3 port 47658 ssh2
2023-11-13T21:07:31.245140+00:00 2e9b0327edc8 sshd[430]: pam_unix(sshd:session): session opened for user test_user(uid=1000) by (uid=0)
2023-11-13T21:07:31.246748+00:00 2e9b0327edc8 sshd[430]: pam_systemd(sshd:session): Failed to connect to system bus: No such file or directory
2023-11-13T21:07:31.250553+00:00 2e9b0327edc8 sshd[430]: pam_env(sshd:session): deprecated reading of user environment enabled
2023-11-13T21:07:31.250579+00:00 2e9b0327edc8 sshd[430]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
2023-11-13T21:07:31.254750+00:00 2e9b0327edc8 sshd[430]: pam_unix(sshd:session): session closed for user test_user
2023-11-13T21:07:32.837992+00:00 2e9b0327edc8 sshd[418]: Failed password for test_user from 172.17.0.3 port 47596 ssh2
2023-11-13T21:07:32.837994+00:00 2e9b0327edc8 sshd[421]: Failed password for test_user from 172.17.0.3 port 47624 ssh2
2023-11-13T21:07:32.840804+00:00 2e9b0327edc8 sshd[419]: Failed password for test_user from 172.17.0.3 port 47604 ssh2
2023-11-13T21:07:32.854773+00:00 2e9b0327edc8 sshd[420]: Failed password for test_user from 172.17.0.3 port 47614 ssh2
2023-11-13T21:07:32.864009+00:00 2e9b0327edc8 sshd[423]: Failed password for test_user from 172.17.0.3 port 47640 ssh2
2023-11-13T21:07:32.864010+00:00 2e9b0327edc8 sshd[422]: Failed password for test_user from 172.17.0.3 port 47626 ssh2
2023-11-13T21:07:32.864011+00:00 2e9b0327edc8 sshd[427]: Failed password for test_user from 172.17.0.3 port 47652 ssh2
2023-11-13T21:07:32.868529+00:00 2e9b0327edc8 sshd[426]: Failed password for test_user from 172.17.0.3 port 47650 ssh2
2023-11-13T21:07:32.868720+00:00 2e9b0327edc8 sshd[431]: Failed password for test_user from 172.17.0.3 port 47660 ssh2
2023-11-13T21:07:32.870566+00:00 2e9b0327edc8 sshd[434]: Failed password for test_user from 172.17.0.3 port 47656 ssh2
2023-11-13T21:07:32.873604+00:00 2e9b0327edc8 sshd[437]: Failed password for test_user from 172.17.0.3 port 47674 ssh2
2023-11-13T21:07:32.913497+00:00 2e9b0327edc8 sshd[442]: Failed password for test_user from 172.17.0.3 port 47696 ssh2
2023-11-13T21:07:33.338502+00:00 2e9b0327edc8 sshd[442]: Connection closed by authenticating user test_user 172.17.0.3 port 47696 [preauth]
2023-11-13T21:07:33.340053+00:00 2e9b0327edc8 sshd[442]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:33.340086+00:00 2e9b0327edc8 sshd[442]: PAM service(sshd) ignoring max retries; 4 > 3
2023-11-13T21:07:34.483527+00:00 2e9b0327edc8 sshd[421]: Connection closed by authenticating user test_user 172.17.0.3 port 47624 [preauth]
2023-11-13T21:07:34.484402+00:00 2e9b0327edc8 sshd[421]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.485416+00:00 2e9b0327edc8 sshd[418]: Connection closed by authenticating user test_user 172.17.0.3 port 47596 [preauth]
2023-11-13T21:07:34.485905+00:00 2e9b0327edc8 sshd[418]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.492732+00:00 2e9b0327edc8 sshd[419]: Connection closed by authenticating user test_user 172.17.0.3 port 47604 [preauth]
2023-11-13T21:07:34.493484+00:00 2e9b0327edc8 sshd[419]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.504003+00:00 2e9b0327edc8 sshd[427]: Connection closed by authenticating user test_user 172.17.0.3 port 47652 [preauth]
2023-11-13T21:07:34.504049+00:00 2e9b0327edc8 sshd[420]: Connection closed by authenticating user test_user 172.17.0.3 port 47614 [preauth]
2023-11-13T21:07:34.505578+00:00 2e9b0327edc8 sshd[420]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.505578+00:00 2e9b0327edc8 sshd[427]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.508387+00:00 2e9b0327edc8 sshd[423]: Connection closed by authenticating user test_user 172.17.0.3 port 47640 [preauth]
2023-11-13T21:07:34.508488+00:00 2e9b0327edc8 sshd[423]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.508565+00:00 2e9b0327edc8 sshd[422]: Connection closed by authenticating user test_user 172.17.0.3 port 47626 [preauth]
2023-11-13T21:07:34.508623+00:00 2e9b0327edc8 sshd[422]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.519025+00:00 2e9b0327edc8 sshd[434]: Connection closed by authenticating user test_user 172.17.0.3 port 47656 [preauth]
2023-11-13T21:07:34.519471+00:00 2e9b0327edc8 sshd[426]: Connection closed by authenticating user test_user 172.17.0.3 port 47650 [preauth]
2023-11-13T21:07:34.519527+00:00 2e9b0327edc8 sshd[431]: Connection closed by authenticating user test_user 172.17.0.3 port 47660 [preauth]
2023-11-13T21:07:34.519585+00:00 2e9b0327edc8 sshd[431]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.519969+00:00 2e9b0327edc8 sshd[434]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.520410+00:00 2e9b0327edc8 sshd[437]: Connection closed by authenticating user test_user 172.17.0.3 port 47674 [preauth]
2023-11-13T21:07:34.520452+00:00 2e9b0327edc8 sshd[426]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:07:34.520537+00:00 2e9b0327edc8 sshd[437]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.3  user=test_user
2023-11-13T21:15:21.163608+00:00 2e9b0327edc8 sshd[34]: exited MaxStartups throttling after 00:07:56, 1 connections dropped
2023-11-13T21:15:22.759186+00:00 2e9b0327edc8 sshd[486]: Accepted password for test_user from 172.17.0.3 port 40098 ssh2
```

Рисунок 2.20 (б) - Вдала авторизація після підбору паролю

Такі сервіси, як 2ip або whois дозволяють отримати усю доступну у відкритих джерелах інформацію про ip адресу, з якої виконувалася атака. А це вже доказова база для правоохоронних органів, яка якщо не прямо, то опосередковано вказуватиме на винуватця, якщо зловмисник не використовував засоби для анонімізації, такі як VPN, VPS або proxy. При використанні подібних інструментів ідентифікація злочинця значно ускладнюється, але все ще не лишається неможливою.

У файлах логів на рисунках 2.20 а-б можна побачити, що перебір паролів виконувався з адреси 172.17.0.3, що збігається з адресою контейнера з ОС kali linux, з якої виконувалася симуляція атаки. Тобто джерело атаки було встановлено вірно.

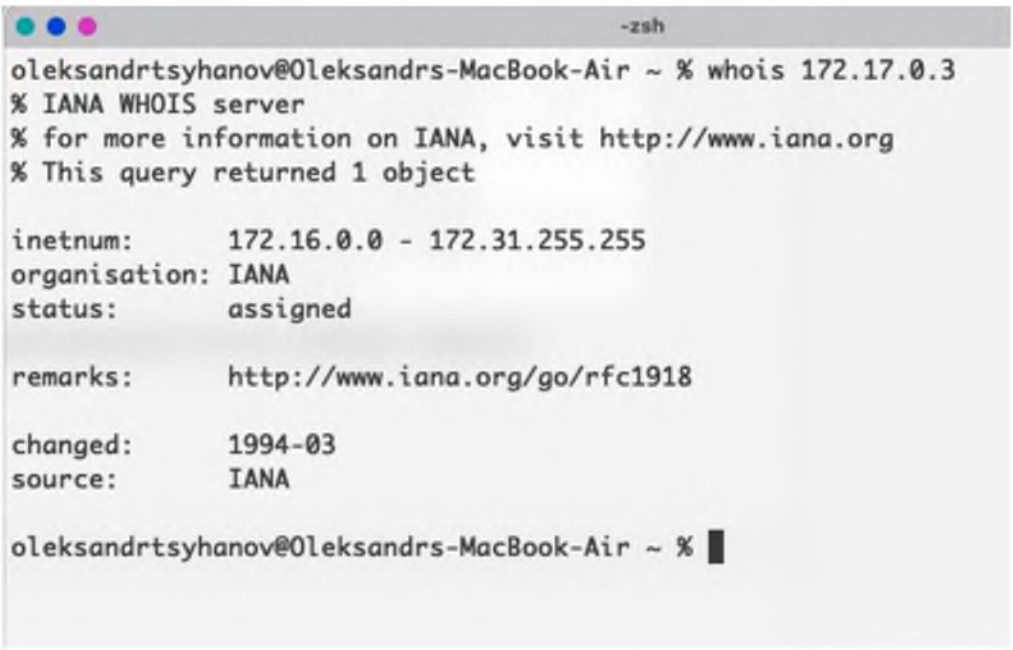

Рисунок 2.21 -Результат запиту до whois

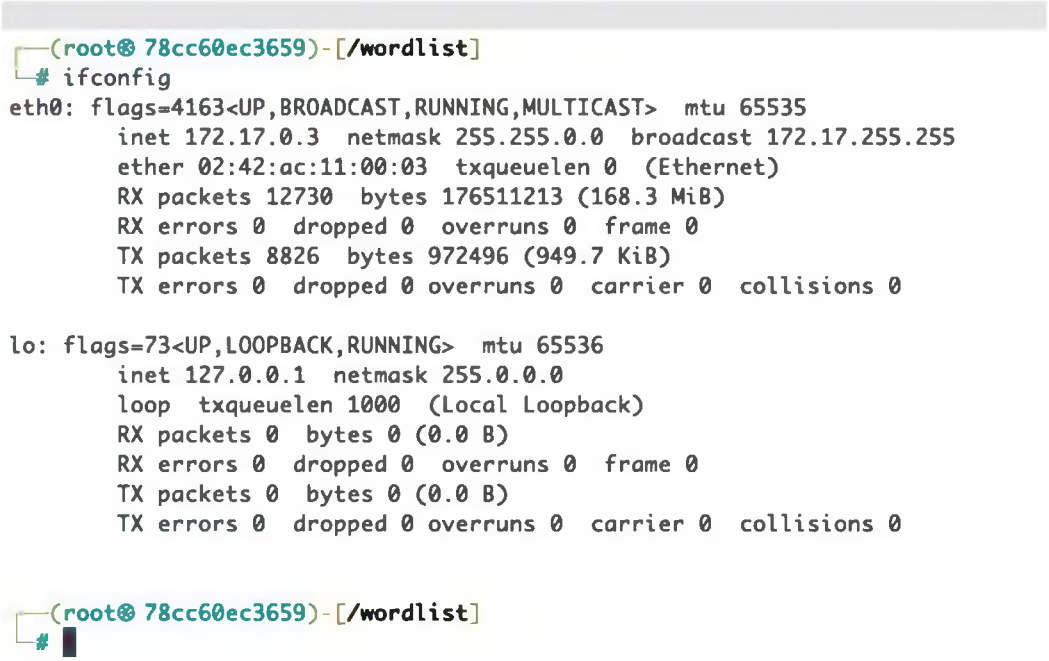

Рисунок 2.22 - Конфігурація мережі контейнера з Kali linux

Окрім розслідування факту втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що покривається статтею 361 кримінального кодексу України, компанії або підприємству слід провести і внутрішнє розслідування, оскільки використання паролів, які були злиті до мережі

має бути заборонене внутрішньою політикою інформаційної безпеки, так як становить ризик несанкціонованого проникнення до внутрішньої мережі. А це в свою чергу несе за собою ризики для конфіденційності, цілісності та доступності інформації. Якщо ж брати до уваги, що подібний інцидент міг трапитися на одному з об'єктів критичної інфраструктури, то це може мати серйозні наслідки навіть на державному рівні.

2.7.Висновки після розслідування інциденту

Після розслідування будь-якого інциденту інформаційної безпеки є етап "Lessons learning", який включає в себе зведення підсумків про те, що призвело до інциденту, як його можна пом'якшити та/або попередити в майбутньому.

На прикладі розглянутого інциденту, підсумки можуть виглядати наступним чином:

«Інцидент стався із системою <назва системи або віртуальної машини> під управлінням операційної системи Debian 12. Протягом інциденту зловмисник намагався підібрати пароль до облікового запису test_user, що обуло видно з відповідних логів у файлі журналів /var/log/auth.log. Після великої кількості невдалих спроб авторизації є дані про успішну авторизацію з тієї ж IP адреси, що і попередні невдалі спроби. Це свідчить про успішний підбір паролю і отримання доступу до цільової машини. Із файлів журналу вдалося встановити, що адреса зловмисника 172.17.0.3 і вона знаходиться в пулі приватних IP адрес. Це означає, що атака проводилася із внутрішньої мережі і необхідно шукати особу, яка використовувала цю адресу.»

У випадку публічної адреси зловмисника можна вказати усю інформацію, яку вдастся знайти в мережі Інтернет. Після збору усіх цифрових доказів і встановлення джерела атаки і за можливості особи, необхідно розробити інструкції для системного адміністратора або адміністратора безпеки для запобігання повторного інциденту.

2.8.Розробка інструкції дій

Найпершим пунктом має бути зміна скомпрометованого паролю, щоб зловмисник не міг ним скористатися в майбутньому. Для unix систем це робиться з допомогою команди passwd <username> з root правами або від користувача root.

Для запобігання подібним інцидентам в майбутньому на інших системах в мережі необхідно перевірити наявність політики паролів і її виконання. Якщо такої політики немає, її необхідно створити. Якщо вона існує і пароль було зламано через недотримання політики, тоді необхідно знайти власника скомпрометованої системи і провести внутрішнє розслідування, з якої причини було встановлено слабкий пароль або яким чином складний пароль могли зламати.

В якості системи зберігання, генерації і перевірки паролів на складність можна використовувати парольні менеджери такі як Last Pass, KeyPass, keychain, Samsung Pass та ін. Якщо архітектура мережі дозволяє (наприклад мережа повністю побудована на Windows), адміністратору слід створити доменні облікові записи для усіх користувачів і налаштувати відповідну політику паролів на контролері домену. Це може бути, наприклад, мінімальна довжина у 12 символів, обов'язкове використання цифр, малих та великих літер (використання спецсимволів за бажанням). Запровадження PAM (privileged access management) також може піти на користь захищеності системи за рахунок обмеженості доступу до сервісу. Згідно даних табл. 2.1 можна зробити висновок, що якщо до 12-символьного паролю із цифр та маленьких літер додати великі букви, то час підбору паролю різко зростає з 2 днів до 24 років. Тому підприємствам варто запроваджувати суворе регулювання складності паролів, які використовують їх співробітники.

Якщо взяти за приклад SSH, на який було змодельовано атаку, він працює на 22-му tcp порту за замовчуванням. Як було згадано на етапі моделювання, такі інструменти як hydra мають базу даних стосовно стандартних портів, на яких працюють різні сервіси, зловмисники також користуються цим стандартом. Для запобігання виявлення потенційної точки входу хорошою практикою буде змінити порт, на якому працює сервіс і обмежити його доступність файрволом.

Для автоматизованого виявлення інцидентів інформаційної безпеки слід запровадити SIEM систему (за наявності відповідних спеціалістів та фінансових можливостей можна подивитися в бік SOAR рішень). Зв'язка із Wazuh та ELK/splunk або платні рішення від IBM (Qradar) або Microsoft (Sentinel) дозволяє в автоматичному режимі (після попереднього налаштування) збирати та аналізувати файли журналів, а також генерувати сповіщення про аномалії всередині мережі.

Таблиця 2.1 - Залежність швидкості підбору паролю від його складу

Кількість символів	Тільки цифри	Букви в нижньому регістрі	Букви в нижньому і верхньому регістрах	Цифри, букви в нижньому і верхньому регістрах	Цифри, букви в нижньому і верхньому регістрах, спецсимволи
4	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
5	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
6	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
7	Миттєво	Миттєво	2 секунди	7 секунд	31 секунда
8	Миттєво	Миттєво	2 хвилини	7 хвилин	39 хвилин
9	Миттєво	10 секунд	1 година	7 годин	2 дні
10	Миттєво	4 хвилини	3 дні	3 тижні	5 місяців
11	Миттєво	2 години	5 місяців	3 роки	34 роки
12	2 секунди	2 дні	24 роки	200 років	3 тис. років
13	19 секунд	2 місяці	1 тис. років	12 тис. років	202 тис. років
14	3 хвилини	4 роки	64 тис. років	750 тис. років	16 млн. років
15	32 хвилини	100 років	3 млн. років	46 млн. років	1 млрд. років
16	5 год	3 тис. років	173 млн. років	3 млрд. років	92 млрд років
17	2 дні	69 тис. років	9 млрд. років	179 млрд. років	7 трлн. років
18	3 тижні	2 млн. років	467 млрд. років	11 трлн. років	438 трлн. років

2.9. Інструкції щодо ліквідації наслідків інциденту

1. Оскільки актуальний пароль було скомпрометованого, його необхідно змінити, щоб в разі повторної атаки зловмисники не мали переваги. Це можна зробити командою “passwd test_user”.

2. Для попередження подібних інцидентів по усій інфраструктурі необхідно мати паролі підвищеної складності скрізь. Для регулювання цієї вимоги створюються політики паролів. Якщо така політики вже існує і є повна впевненість, що вона виконується, описаний інцидент має стати причиною перегляду політики. Складність паролю має бути такою, щоб згідно табл. 2.1 зловмисникам знадобилося не менше 1 року на підбір паролю.

3. Після впровадження або редагування існуючої політики паролів необхідно провести аудит усіх систем в мережі і переконатися, що всі паролі відповідають новій політиці.

4. Для зручності зберігання і генерації паролів за заданими параметрами має сенс використовувати менеджери паролів. Прикладом подібних сервісів можуть бути LastPass, 1Password, KeePass, Samsung Pass і т.п.

5. Для перешкоджання виявлення інтерактивного сервісу (такий, що може взаємодіяти з користувачем і має поля для вводу данних) необхідно змінити стандартний порт атакованого сервісу і впровадити подібне рішення по всій організації. Для SSH:

- У файлі /etc/ssh/sshd_config розкоментувати рядок #Port 22 і присвоїти інше значення (наприклад, Port 10022).
- Перезапустити сервіс командою systemctl restart ssh або service ssh restart (для Systemd і System V відповідно).
- Якщо переналаштований сервіс використовується в бізнес процесах, не обхідно внести відповідні корегування.

6. Якщо зловмисник сканує усі 65535 портів, то навіть у випадку переносу порту сервіс з великою вірогідністю буде знайдено, тому необхідно визначити, хто і для чого користується цим сервісом і обмежити його доступність

тільки для визначеного кола людей. Для подібних задач необхідно налаштувати файрвол. Найпоширенішим для linux систем є iptables.

7. Для мінімальної протидії вторгненням, накшталт перебору паролів, необхідно встановити і налаштувати fail2ban або його аналог для windows систем. Необхідно прослідкувати, щоб його поточних налаштувань було достатньо. Якщо у випадку повторної атаки перебором зловмиснику все ще вдається пробитися крізь fail2ban (помічено саме однакову адресу-джерело атаки), необхідно зменшити кількість невдалих спроб, після яких адреса блокуватиметься і збільшити час блокування.

8. Для зручності збору і подальшого аналізу логів, а також можливості сповіщення у випадку аномалій необхідно розгорнути та налаштувати SIEM або SOAR систему.

2.10. Висновки

В розділі було змодельовано поширений вузол інфраструктури, який може бути частиною будь-якої інформаційно-комунікаційної системи на будь-якому рівні, а саме linux система з SSH сервером. Моделювання проводилося з допомогою програмного комплексу для контейнеризації - docker.

На цьому вузлі для спрощення експерименту було створено тестового користувача і умисно назначено йому слабкий пароль. Після чого змодельовано brute-force атаку на SSH для цього користувача.

Після виявлення інциденту було проведено криміналістичне розслідування шляхом аналізу файлів журналів /var/log/auth.log і встановлення адреси, з якої виконувалася атака. По завершенні розслідування було складено план щодо нейтралізації наслідків інциденту.

3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1.Розрахунок капітальних витрат

Капітальні інвестиції - це кошти, призначені для створені і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До фіксованих капітальних витрат відносять:

– вартість розробки проекту інформаційної безпеки (розробка схем пристроїв, політики функціонування системи тощо);

– витрати на залучення зовнішніх консультантів;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– вартість створення основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

3.1.1. Визначення трудомісткості розробки та опрацювання

Трудомісткість виконання проекту визначається тривалістю кожної робочої операції:

$t_{тз}$- тривалість складання ТЗ, літературних джерел за темою, тощо;

$t_{в}$ - тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ - тривалість розробки алгоритму практичної частини

$t_{пр}$ - тривалість виконання робіт за складеним алгоритмом

$t_{опр}$- тривалість опрацювання;

$t_{д}$ - тривалість підготовки технічної документації (процедур та опису проведених робіт)

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{а}} + t_{\text{пр}} + t_{\text{опр}} + t_{\text{д}} \quad (3.1)$$

Складові трудомісткості визначаються на підставі умовної кількості операторів у програмному продукті Q (з урахуванням можливих уточнень у процесі роботи над алгоритмом і програмою).

Умовна кількість операторів у програмі:

$$Q = q \cdot c(1 + p), \text{ штук} \quad (3.2)$$

де q - очікувана кількість операторів - за цю кількість було прийнято кількість елементарних операцій для моделювання і розслідування інсценованого інциденту інформаційної безпеки;

c - коефіцієнт складності моделювання;

p - коефіцієнт корекції алгоритму в процесі виконання;

Коефіцієнт складності програми $\boldsymbol{c}$ визначає відносну складність програми щодо типового завдання, складність якого дорівнює одиниці. Діапазон його зміни - 1,25…2,0.

Коефіцієнт корекції $\boldsymbol{p}$ визначає збільшення обсягу робіт за рахунок внесення змін в алгоритм або програму внаслідок уточнення технічного завдання. Його величина знаходиться в межах 0,05…0,1, що відповідає внесення 3…5 корекцій і переробці 5-10% процесу моделювання.

$$Q = 12 \cdot 1{,}25\ (1 + 0{,}05) = 15{,}75 \approx 16$$

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення ТЗ і кваліфікації інженера з безпеки можливо оцінити за формулою

$$t_{\text{в}} = \frac{Q \cdot B}{(75 \ldots 85) \cdot k}, \text{ годин} \quad (3.3)$$

де В - коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, В = 1,2…1,5;

k - коефіцієнт, що враховує кваліфікацію інженера з безпеки і визначається за фахом:

- до 2 років - 0,8;
- від 2 до 3 років - 1,0;
- від 3 до 5 років - 1,1…1,2;
- від 5 до 7 років - 1,3…1,4;
- понад 7 років - 1,5…1,6

Результат розрахунку за формулою 3.3:

$t_{\text{в}} = \frac{16 \cdot 1{,}2}{80 \cdot 1} = 2{,}4 \text{ години} = 2 \text{ год } 24 \text{ хв}$

Тривалість розробки алгоритму:

$$t_{\text{а}} = \frac{Q}{(20 \ldots 25)k} = \frac{16}{23 \cdot 1} = 0{,}7 \text{ годин} = 42 \text{ хв} \quad (3.4)$$

Тривалість виконання робіт за складеним алгоритмом:

$$t_{\text{пр}} = \frac{Q}{(20 \ldots 25) \cdot k} = \frac{16}{23 \cdot 1} = 0{,}7 \text{ годин} = 42 \text{ хв} \quad (3.5)$$

Тривалість опрацювання на ПК

$$t_{\text{опр}} = \frac{1{,}5Q}{(4 \ldots 5) \cdot k} = \frac{1{,}5 \cdot 16}{4{,}5 \cdot 1} = 5{,}3 \text{ годин} = 5 \text{ год } 18 \text{ хв} \quad (3.6)$$

Тривалість підготовки технічної документації:

$$t_д = \frac{Q}{(15 \dots 20) \cdot k} + \frac{Q}{(15 \dots 20) \cdot k} \cdot 0{,}75 = \frac{16}{17 \cdot 1} + \frac{16}{17 \cdot 1} \cdot 0{,}75 \quad (3.7)$$
$$= 0{,}94 + 0{,}71 = 1{,}65 \text{ годин} = 1 \text{ год } 39 \text{ хв}$$

Загальна трудомісткість проекту складатиме:

$$t = 2 + 2{,}4 + 0{,}7 + 0{,}7 + 5{,}3 + 1{,}65 = 12 \text{ год } 45 \text{ хв} \quad (3.8)$$

при витрачених 2 годинах на кладання ТЗ.

3.1.2. Розрахунок витрат на моделювання

Витрати на моделювання $K_{пз}$ складаються з витрат на заробітню плату виконавця $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК $З_{мч}$.

$$K_{пз} = З_{зп} + З_{мч} = 1410 + 44{,}2 = 1454{,}2 \text{ грн} \quad (3.9)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \cdot З_{пр} = 12{,}75 \cdot 110{,}59 = 1410 \text{ грн} \quad (3.10)$$

де t - загальна тривалість створення ПЗ, годин;

$З_{пр}$ - средньогодинна заробітна плата інженера з інформаційної безпеки з нарахуваннями, грн/годину. При заробітній платі інспектора кіберполіції 19464

грн/міс і 176 годинному робочому місяці було прийнято $З_{пр} = \frac{19464}{176} = 110{,}59$ грн/год. [13]

Вартість машинного часу для виконання робіт визначається за формулою:

$$З_{мч} = (t_{опр} + t_д) \cdot C_{мч} = (5{,}3 + 1{,}65) \cdot 6{,}36 = 44{,}2 \text{ грн} \quad (3.11)$$

де $t_{опр}$ - трудомісткість опрацювання, годин;

$t_д$ - трудомісткість підготовки документації на ПК, годин;

$C_{мч}$ - вартість 1 години машинного часу ПК, грн/година;

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{K_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн} \quad (3.12)$$

де P - встановлена потужність ПК, кВт, $P = 30$ Вт $= 0{,}03$ кВт;

$C_е$ - тариф на електричну енергію, грн/кВт · годин $C_е = 2{,}64$;

$Ф_{зал}$ - залишкова вартість ПК на поточний рік, грн $Ф_{зал} = 31000$;

$Н_а$ - річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ - річна норма амортизації на ліцензійне ПЗ, частки одиниці;

$K_{лпз}$ - вартість ліцензійного ПЗ, грн

$F_р$ - річний фонд робочого часу (за 40-годинного робочого тижня $F_р = 1920$).

Річна норма амортизації при початковій вартості ПК 1850 доларів США, залишковій вартості 849 доларів США і терміні експлуатації ПК 1,5 роки становить:

$$Н_а = \frac{1850}{\frac{1850 - 849}{1{,}5}} = 0{,}36 \quad (3.13)$$

Час, необхідний для налагодження процесу моделювання:

$$t_{\text{нал}} = t_{\text{опр}} + t_{\text{д}} = 5{,}3 + 1{,}65 = 6{,}95 \text{ год} = 6 \text{ год } 57 \text{ хв} \quad (3.14)$$

За використання повністю безкоштовного ПЗ (вартість ОС входила у вартість ноутбука, оскільки вона передвстановлена):

$$C_{\text{мч}} = 0.03 \cdot 6{,}95 \cdot 2{,}64 + \frac{31000 \cdot 0{,}36}{1920} = 6{,}36, \text{грн}$$

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта практики інформаційної безпеки складають:

$$K = K_{\text{пр}} + K_{\text{зпз}} + K_{\text{пз}} + K_{\text{аз}} + K_{\text{навч}} + K_{\text{н}} \quad (3.15)$$
$$= 1454{,}2 + 0 + 0 + 26363{,}55 + 0 = 27817{,}75 \text{ грн}$$

де $K_{\text{пр}}$ - вартість проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$K_{\text{зпз}}$ - вартість закупівель ліцензійного основного й додаткового ПЗ, тис. грн;

$K_{\text{пз}}$ - вартість створення основного й додаткового ПЗ, тис. грн. Оскільки в межах проекту створення ПЗ не виконувалося, то розрахована раніше його вартість не враховується.

$K_{\text{аз}}$ - вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$K_{\text{навч}}$ - вартість навчання технічних фахівців і обслуговуючого персоналу, тис. грн. Мінімальна вартість підготовки до профільної сертифікації CHFI (Computer Hacking Forensic Investigator) коштує $718, що становить 26363,55 гривень на момент написання кваліфікаційної роботи. Вартість іспиту входить до ціни підготовки. Також існує можливість здачі іспиту без підготовки, але розглядається варіант з підготовкою спеціаліста з базовими знаннями.

$К_н$ - витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. Оскільки ніякого обладнання або налагодження системи в процесі розслідування цифрових інцидентів не відбувається, цю складову можна ігнорувати.

3.2. Розрахунок поточних (експлуатаційних) витрат

Річні експлуатаційні витрати складають:

$$С = С_в + С_к + С_{ак} = 0{,}21 \cdot 27817{,}75 + 556{,}36 + 0{,}46 \cdot 27817{,}75 = 19194{,}25 \text{ грн.} \quad (3.16)$$

Статистично витрати на відновлення системи складають 21% від капітальних витрат, а активність користувача - 46%.

Витрати на керування системою інформаційної безпеки:

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос} = 0 + 0 + 0 + 0 + 0 + 556{,}36 = 556{,}36 \text{ грн.} \quad (3.17)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо ($С_н$). $С_н = 0$.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$) складає 0 грн, оскільки необхідність в такому персоналі відсутня.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата - в розмірі 8-10% від основної заробітної плати.

До річного фонду заробітної плати додається єдиний внесок на загальнообов'язкове державне соціальне страхування - консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності. Розмір єдиного внеску визначається на підставі

встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$) дорівнюватиме 0, оскільки в роботі не використовується додаткової апаратури.

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу $С_о$ прийнято нульовою, оскільки в роботі мова йде про одного інженера з цифрової криміналістики, а вартість його навчання була врахована на попередніх етапах

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються за даними організації або у відсотках від вартості капітальних витрат (1-3%).

$$С_{тос} = 0{,}02 \cdot K = 0{,}02 \cdot 27\,817{,}75 = 556{,}36 \text{ грн.} \quad (3.18)$$

Витрати викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, користуючись даними табл. 1 про вагові частки статей витрат у сукупній вартості системи інформаційної безпеки.

3.3. Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі

3.3.1. Оцінка величини збитку

Якщо кожна вдала або невдала кібератака буде розслідувана згідно загальноприйнятих стандартів або процедур, складених на етапі підготовки документації, шанс повторної атаки на вузол або сегмент корпоративної мережі знижується до 0, оскільки план дій, який створюється по закінченню розслідування спрямований на закриття потенційного вектора атаки.

Враховуючи той факт, що усі кібератаки спрямовані на отримання неправомірної вигоди шляхом крадіжки та продажу на чорному ринку персональних даних або використання обчислювальних потужностей підприємства

для наживи (майнінг криптовалюти), збитки від зламу можна поділити на 3 категорії:

1. Втрата персональних даних клієнтів або громадян (для об’єктів КІ);
2. Втрата контролю над власними обчислювальними системами та внаслідок цього нераціональне використання ресурсів обчислювальної техніки.
3. Простій вузла або сегмента корпоративної мережі.

За пункт 1 згідно статті 188-39 Кодексу про адміністративні правопорушення передбачена адміністративна відповідальність за недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, тягне за собою накладення штрафу на громадян від 1700 до 8500 грн. і на посадових осіб, громадян - суб'єктів підприємницької діяльності - від 5100 грн. до 17000 грн.

Вищезазначене порушення, вчинене повторно протягом року, за яке особу вже було піддано адміністративному стягненню, тягне за собою накладення штрафу від 17000 грн. до 34000 грн.[14]

Пункт 2 за відсутності лімітів на використання потужностей або зняття коштів за користування хмарними сервісами тягне за собою 2 сценарії:

1. Простій вузла внаслідок відмови в обслуговуванні (тобто 3-я категорія наслідків) для серверів, що обслуговуються безпосередньо підприємством.
2. Необмежене використання хмарних обчислювальних потужностей, що в наслідку може привести до банкрутства і закриття компанії.

Пункт 3 для приватних компаній менш критичний, оскільки вони мають резервні потужності на випадок простою вузла або сегменту мережі. Це не несе за собою додаткових матеріальних витрат, оскільки в бюджет компанії вже закладене їх обслуговування навіть у стані простою. Для сектору КІ цей фактор може бути вже більш критичним, якщо резервних потужностей з якоїсь немає. Наслідки подібних подій оцінюються на рівні функціонування державної інфраструктури.

За відсутності практики з розслідування цифрових злочинів можна припустити що на підприємстві або об'єкті КІ ніхто не займався налагодженням інформаційної безпеки. Таким чином, ризик повторного зламу протягом року можна вважати досить високим. У випадку втрати персональних даних маємо втрати підприємства у вигляді штрафу:

$$Ш = П_1 + \sum П_n \tag{3.19}$$

де Ш - сума штрафу, який має виплатити підприємство, грн

$П_1 = 1700 \dots 8500$ грн - сума штрафу підприємства в разі 1-го правопорушення протягом року

$П_n = 17000 \dots 34000$ грн - штраф за кожне повторне правопорушення протягом року.

У випадку 2-х правопорушень протягом року підприємство в середньому мало б заплатити: $Ш = 5100 + 25500 = 30600$ грн.

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} = 0 + 565{,}23 + 0 = 565{,}23 \text{ грн.} \tag{3.20}$$

де $П_{ви}$ - витрати на повторне уведення інформації, грн

$П_{пв}$ - витрати на відновлення вузла або сегмента корпоративної мережі, грн

$П_{зч}$ - вартість заміни устаткування або запасних частин, грн

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в = \frac{2 \cdot 12435}{176} \cdot 4 = 565{,}23 \text{ грн.} \quad (3.21)$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складає:

$$B = Ш + П_{пв} + x = 30600 + 565{,}23 = 31165{,}23 \text{ грн.} + x \quad (3.22)$$

де х - невраховані збитки від простою, які залежать від специфіки бізнесу, або вартості репутаційних збитків.

3.3.2. Загальний ефект від впровадження практики інформаційної безпеки

Загальний ефект від впровадження практики інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C = 31165{,}23 \cdot 0{,}9 - 19194{,}25 = 8854{,}25 \text{ грн.} \quad (3.23)$$

де В - загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн

R - очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці

С - щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн

3.4. Вивчення та аналіз показників економічної ефективності практики інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу наступних показників:

а) сукупна вартість володіння (ТСО);

б) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

в) термін окупності капітальних інвестицій T_o.

Ключовою перевагою показника ТСО є те, що він дозволяє зробити висновки про доцільність реалізації проекту в області інформаційної безпеки на підставі оцінки одних тільки витрат.

Показник сукупної вартості володіння (ТСО) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі важко або неможливо визначити у вартісній формі.

У цьому випадку необхідно порівняти сукупну вартість володіння, розраховану для двох варіантів проектного рішення щодо створення або удосконалення системи інформаційної безпеки, і вибрати варіант із найменшою з них.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K} = \frac{8854{,}25}{27817{,}75} = 0{,}32 \tag{3.24}$$

де Е - загальний ефект від впровадження системи інформаційної безпеки

К - капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Проект системи інформаційної безпеки визнається доцільним за умови

$$ROSI > E_{\text{н}} \tag{3.25}$$

де $E_{\text{н}}$ - бажаний показник ефективності.

Якщо організація здійснює фінансування капітальних інвестицій у систему інформаційної безпеки за рахунок позикових коштів (банківського кредиту), то в якості бажаного значення $E_{\text{н}}$ варто приймати величину плати за кредит (кредитної ставки) $N_{\text{кр}}$.

Проект визначається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину банківської кредитної ставки з урахуванням інфляції:

$$ROSI > (N_{\text{кр}} + N_{\text{інф}})/100 \quad (3.26)$$

$$ROSI > (18 + 5{,}1)/100$$

$$0{,}32 > 0{,}231$$

де $N_{\text{кр}}$ - банківська депозитна ставка, %

$N_{\text{інф}}$ - річний рівень інфляції, %

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{K}{E} = \frac{1}{0{,}32} = 3{,}125 \text{ роки} = 3 \text{ роки } 1{,}5 \text{ міс} \quad (3.27)$$

3.5. Висновки

Згідно з наведеними розрахунками, можна зробити висновок, що впровадження практики розслідування інцидентів інформаційної безпеки на підприємстві буду економічно доцільним.

При капітальних витратах 27817,75 грн ефект від впровадження практики цифрової криміналістики цифрових інцидентів становитиме щонайменше 8854,25 грн. Отже коефіцієнт повернення інвестицій складатиме мінімум 0,32 грн на кожну 1 грн вкладень.

Таким чином впровадження практики розслідування інцидентів інформаційної безпеки для підприємства окупиться за 3,125 роки або 3 роки і 1,5 місяці. Цей термін (як і коефіцієнт повернення інвестицій) може варіюватися в залежності від специфіки конкретно взятого підприємства і вартості даних, з якими воно працює.

ВИСНОВКИ

Застосування методів цифрової криміналістики в розслідуванні інцидентів кібербезпеки на об’єктах критичної інфраструктури виявилося ефективним та необхідним. Досліджені методи дозволяють збирати достовірну інформацію, виявляти слабкі місця в системах безпеки та ефективно реагувати на кібератаки.

Обраний методологічний підхід до аналізу змодельованого інциденту сприяв визначенню винуватців та розкриттю причин інциденту. За результатами дослідження була зібрана доказова база та встановлені причини, що дозволяє визначити підходи до підвищення рівня кібербезпеки та запобігання подібним інцидентам у майбутньому.

Усунення наслідків кіберінциденту потребує комплексного підходу та використання рекомендацій, розроблених на основі отриманих результатів дослідження. Важливою є взаємодія між фахівцями з цифрової криміналістики, інженерами з кібербезпеки та представниками об'єктів критичної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Українська Вікіпедія. "Об'єкти критичної інфраструктури." [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Об%27єкти_критичної_інфраструктури

2. Законодавча база Верховної Ради України. "Закон України від 15.04.2020 № 1882-IX 'Про критичну інфраструктуру'." [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text

3. Портал правової інформації "LegalAid." "Кіберполіція. Кібербезпека України." [Електронний ресурс]. Режим доступу: https://wiki.legalaid.gov.ua/index.php/Кіберполіція._Кібербезпека_України

4. Рада національної безпеки і оборони України. "Проект Стратегії кібербезпеки України." [Електронний ресурс]. Режим доступу: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

5. Lepide Blog. "The 15 Most Common Types of Cyber Attacks." [Електронний ресурс]. Режим доступу: https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/

6. Spiceworks. "What Is Digital Forensics?" [Електронний ресурс]. Режим доступу: https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-digital-forensics/

7. GeeksforGeeks. "Computer Forensics Techniques." [Електронний ресурс]. Режим доступу: https://www.geeksforgeeks.org/computer-forensics-techniques/

8. Studfile. “Модель порушника інформаційної безпеки” [Електронний русурс]. Режим доступу: https://studfile.net/preview/8875886/page:12/

9. OWASP. “ Top 10 Web Application Security Risks” [Електронний русурс]. Режим доступу: https://owasp.org/www-project-top-ten/

10. Ekran Systems. “ Brute Force Attacks: How to Detect and Prevent Them” [Електронний ресурс]. Режим доступу: https://www.ekransystem.com/en/blog/brute-force-attacks

11. Wikipedia. “ Docker (software)” [Електронний ресурс]. Режим доступу: https://en.wikipedia.org/wiki/Docker_(software)

12. Kali. “ Tool Documentation: hydra Usage Example” [Електронний ресурс]. Режим доступу: https://www.kali.org/tools/hydra/

13. AIN. “Кіберполіція має вакансії для айтівців. Зарплата від 19 000 грн” [Електронний ресурс]. Режим доступу: https://ain.ua/2023/02/23/kiberpolicziya-maye-vakansiyi-dlya-ajtivcziv-zarplata-vid-19-000-grn/

14. Юрліга. “Персональні дані: використання, захист і відповідальність - що потрібно знати” [Електронний ресурс]. Режим доступу: https://jurliga.ligazakon.net/news/201367_personaln-dan-vikoristannya-zakhist--vdpovdalnst---shcho-potrbno-znati#:~:text=до%2034%20000%20грн.,700%20до%208%20500%20грн

15. ISO/IEC 27000:2018, Information technology - Security techniques - Information security management systems - Overview and vocabulary.

16. ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements.

17. ISO/IEC 27032:2012, Information technology - Security techniques - Guidelines for cybersecurity.

18. Кваліфікаційна робота магістра: методичні вказівки / Гусєв О.Ю., Корнієнко В.І., Магро В.І., Тимофєєв Д.С. Дніпро: Національний технічний университет «Дніпровська політехніка», 2022. 34 с.

19. Шереметьєва І.В., Пілова Д.П., Романюк Н.М. Методичні вказівки до виконання економічної частини дипломного проекту: методичні вказівки Дніпро: Національний технічний университет «Дніпровська політехніка», 2017. 17 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	27	
6	А4	2 Розділ	27	
7	А4	3 Розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Титульна сторінка.doc
2. Завдання.doc
3. Реферат.doc
4. Список умовних скорочень.doc
5. Зміст.doc
6. Вступ.doc
7. Розділ 1.doc
8. Розділ 2.doc
9. Розділ 3.doc
10. Висновки.doc
11. Перелік посилань.doc
12. Додаток А.doc
13. Додаток Б.doc
14. Додаток В.doc
15. Додаток Г.doc
16. Презентація.pptx

ДОДАТОК В

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («Відмінно»).

Керівник розділу _____ доц. Пілова Д.П.
(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу магістра на тему: Застосування методів цифрової криміналістики при розслідувані інцидентів кібербезпеки на об'єктах критичної інфраструктури

ст. гр. 125м-22-2 Циганова Олександра Олеговича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 83 сторінках та містить 24 рисунків, 1 таблиць, 19 джерел та 4 додатка.

Мета кваліфікаційної роботи - дослідити наявні методи цифрової криміналістики і обрати комплексне рішення для розслідування інциденту.

За допомогою обраних методів зібрати доказову базу, описати інцидент, що стався і запропонувати план дій щодо усунення наслідків інциденту.

В першому розділі проаналізовано сучасні загрози для критичної інфраструктури, потенційні наслідки від успішних атак на її мережі і вузли, а також існуючі методи цифрової криміналістики розслідування інцидентів.

У спеціальному розділі було описано процес створення тестового полігону з двох docker-контейнерів, на якому в подальшому проведено моделювання інциденту кібербезпеки. За мотивами змодельованого інциденту було проведено розслідування методами цифрової криміналістики, відновлено картину подій, що сталися, зібрано доказову базу та надано інструкції щодо нейтралізації наслідків інциденту.

В економічному розділі було проведено розрахунки капітальних витрат на впровадження практики розслідування цифрових злочинів та терміну окупності інвестицій.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник