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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Виблого Сергія Руслановича*

академічної групи *125м-22з-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка алгоритму проведення тесту на проникнення при аудиті інформаційної безпеки підприємства*

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

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Виблому Сергію Руслановичу*** **академічної групи** ***125м-22з-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка алгоритму проведення тесту на проникнення при аудиті інформаційної безпеки підприємства***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Постановка задачі	02.10.2023
Розділ 2	Спеціальна частина	06.11.2023
Розділ 3	Економічна частина	04.12.2023

Завдання видано _____ Сафаров О.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Виблий С.Р.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка складається з: 99 с., 8 рис., 6 табл., 4 додатків, 14 джерел.

Об’єкт дослідження: аудит інформаційної безпеки.

Мета кваліфікаційної роботи: сприяння реалізації процесу розробки тестування на проникнення шляхом розробки алгоритму тесту на проникнення.

У роботі проаналізовано процес розробки алгоритму на проникнення та сучасні методи активного аудиту.

У спеціальній частині створено узагальнену модель алгоритму проведення тесту на проникнення та показані рекомендації до його проведення.

В економічному розділі проведено розрахунок вартості проєктування та проведення тесту на проникнення у вже існуючу інформаційну систему та зроблено висновок щодо доцільності проведення тесту на проникнення.

Наукова новизна полягає у створенні узагальненого алгоритму проведення тесту на проникнення з метою підвищення рівня інформаційної безпеки підприємства та зменшення фінансових затрат на проведення експертної оцінки.

АЛГОРИТМ ПРОВЕДЕННЯ ТЕСТУ НА ПРОНИКНЕННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, АНАЛІЗ ВРАЗЛИВОСТЕЙ, ОБРОБКА ВРАЗЛИВОСТЕЙ

THE ABSTRACT

Explanatory notes consist of 99 pages, 8 pictures, 6 table, 4 appendices, 14 sources.

Objective: to improve the efficiency of investigation of incidents of information security.

Object of study: information security audit.

Objective of qualification work: facilitating the implementation of the penetration testing development process by developing a penetration test algorithm.

The research analyzes the process of developing of the penetration testing algorithm and modern methods of active audit.

The special part includes the development of a generalized model algorithm of the penetration test and shows recommendations for its process.

The economic section includes calculation of the cost of development and integration of the penetration test to an existing information system. The conclusion about the appropriateness of the penetration test was made.

The scientific novelty lies in creation of a generalized algorithm of penetration testing in order to improve information security and reduce the financial costs of expert's evaluation.

PENETRATION TESTING ALGORITHM, INFORMATIONAL SECURITY, VULNERABILITY ANALYSIS, TREATMENT OF VULNERABILITY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІБ – інформаційна безпека;

ІТ – інформаційні технології;

ПЗ – програмне забезпечення;

СІБ – система інформаційної безпеки;

BGP – Border Gateway Protocol – протокол граничного шлюзу;

DHCP – Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла;

DNS – Domain Name System – система доменних імен;

EIGRP – Enhanced Interior Gateway Routing Protocol – протокол маршрутизації;

HSRP – Hot Standby Router Protocol, Hot Standby Redundancy Protocol – протокол сімейства FHRP (First Hop Redundancy Protocol);

ICMP – Internet Control Message Protocol – міжмережевий протокол керуючих повідомлень;

OSPF – Open Shortest Path First – протокол динамічної маршрутизації;

RIP – Routing Information Protocol – протокол маршрутної інформації;

SSID – Service Set Identifier –- ідентифікатор бездротової мережі;

URL – Uniform Resource Locator – єдиний вказівник ресурсів;

VPN – Virtual Private Network – віртуальна приватна мережа;

VRRP – Virtual Router Redundancy Protocol – віртуальний протокол надмірної маршрутизації.

ЗМІСТ

ВСТУП

Інформаційна безпека стає все більш пріоритетною сферою для розвитку підприємств. Поважаюча свою працю компанія замислюється над тим, наскільки якісною і ефективною є власна інформаційна безпека, адже зневажливе ставлення до цього питання може призвести до значних збитків, а то й краху підприємства.

Проте інформаційна безпека – це виключно комплексний процес, що вимагає участі всіх співробітників підприємства, тимчасових і постійних, а також третіх осіб, постачальників, контрагентів, партнерів задля надійного використання інформаційних технологій, обслуговування обладнання і каналів зв'язку, створення документації бізнес-процесів - тобто організації ефективної системи управління інформаційної безпеки.

Різноманітність і постійна зміна загроз ускладнює управління ними, при цьому вірогідність їх реалізації не зменшується. Проведення аудиту інформаційної безпеки, який є необхідним інструментом на кожному підприємстві зменшує вірогідність реалізації вразливостей. Проте досягнення високої ефективності процесу управління ІБ вимагає наявності висококваліфікованих спеціалістів в даній галузі та можливості аналізувати велику кількість несистематизованої інформації.

Розв’язанням проблеми ефективного управління інформаційної безпеки є регулярне проведення тесту на проникнення, який сьогодні дозволяє застосовувати передові технології обробки та збереження інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Поняття аудиту інформаційної безпеки

Визначення аудиту безпеки в загальному випадку можна описати як процес збору та аналізу інформації про ІБ для якісної або кількісної оцінки рівня її захищеності від атак зловмисників. Існує безліч випадків, коли доцільно проводити аудит безпеки. Це робиться, зокрема, при підготовці технічного завдання на проєктування та розробку системи захисту інформації та після впровадження системи безпеки для оцінки рівня її ефективності. Можливий аудит, спрямований на приведення діючої системи безпеки у відповідність вимогам українського або міжнародного законодавства. Аудит може також призначатися для систематизації та впорядкування існуючих заходів захисту інформації або для розслідування інциденту, пов'язаного з порушенням інформаційної безпеки.

Як правило, для проведення аудиту залучаються зовнішні компанії, які надають консалтингові послуги в області інформаційної безпеки. Ініціатором процедури аудиту може стати керівництво підприємства, служба автоматизації або служба інформаційної безпеки. У ряді випадків аудит також проводиться на вимогу страхових компаній або регулюючих органів. Аудит безпеки виконується групою експертів, чисельність і склад якої залежить від цілей і завдань обстеження, а також від складності об'єкта оцінки.

1.1.1 Види аудиту безпеки

Можна виділити наступні основні види аудиту інформаційної безпеки:

- експертний аудит безпеки, в ході якого виявляються недоліки в системі заходів захисту інформації на основі досвіду експертів, що беруть участь у процедурі обстеження;
- оцінка відповідності рекомендаціям міжнародного стандарту ISO 27002;

- інструментальний аналіз захищеності ІС, спрямований на виявлення та усунення вразливостей програмно-апаратного забезпечення системи;
- тест на проникнення, аналіз вразливостей і моделювання атак зловмисника;
- комплексний аудит, що включає в себе всі перераховані вище форми проведення обстеження.

Будь-який з перелічених видів аудиту може проводитися окремо або в комплексі, в залежності від тих завдань, які вирішує підприємство. В якості об'єкта аудиту може виступати як ІС компанії в цілому, так і її окремі сегменти, в яких обробляється інформація, що підлягає захисту.

1.1.2 Зовнішній і внутрішній аудит

Зовнішній аудит - це, як правило, разовий захід, що проводиться з ініціативи керівництва організації або акціонерів. Зовнішній аудит рекомендується (а для ряду фінансових установ та акціонерних товариств потрібно) проводити регулярно.

Внутрішній аудит являє собою безперервну діяльність, яка здійснюється на підставі документа, зазвичай носить назву "Положення про внутрішній аудит", і згідно з планом, підготовка якого здійснюється підрозділом внутрішнього аудиту та затверджується керівництвом організації. Аудит безпеки інформаційних систем є однією зі складових IT-аудиту.

Цілями проведення аудиту безпеки є:

- аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів ІС;
- оцінка поточного рівня захищеності ІС;
- локалізація вузьких місць в системі захисту ІБ;
- оцінка відповідності ІС існуючим стандартам в галузі інформаційної безпеки;
- вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС;

– представлені аудитору рапорти про інциденти СІБ повинні містити документацію про так звані "слабкі точки" СІБ.

У число додаткових завдань, що стоять перед внутрішнім аудитором, крім надання допомоги зовнішнім аудиторам, можуть також входити:

– розробка політик безпеки та інших організаційно-розпорядчих документів щодо захисту інформації та участь у їх впровадженні в роботу організації;
– постановка завдань для IT-персоналу, що стосуються забезпечення захисту інформації;
– участь у навчанні користувачів і обслуговуючого персоналу з питань забезпечення інформаційної безпеки;
– участь у розборі інцидентів, пов'язаних з порушенням інформаційної безпеки;
– інші завдання.

1.2 Активний аудит

Одним з найпоширеніших видів аудиту є активний аудит. Це дослідження стану захищеності інформаційної системи з погляду хакера (або якогось зловмисника, який володіє високою кваліфікацією в галузі інформаційних технологій).

Найчастіше компанії-постачальники послуг активного аудиту іменують його інструментальним аналізом захищеності, щоб відокремити даний вид аудиту від інших.

Суть активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів здійснюється збір інформації про стан системи мережевого захисту. Під станом системи мережевого захисту розуміються лише ті параметри і настройки, використання яких допомагає хакеру проникнути в мережі й завдати шкоди компанії.

При здійсненні даного виду аудиту на систему мережевого захисту моделюється як можна більша кількість мережевих атак, які може виконати хакер. При цьому аудитор штучно ставиться саме в ті умови, в яких працює хакер, - йому надається мінімум інформації, тільки та, яку можна роздобути у відкритих джерелах.

Природно, атаки тільки моделюються і не надають будь-якого деструктивного впливу на інформаційну систему. Їх різноманітність залежить від використовуваних систем аналізу захищеності та кваліфікації аудитора. Результатом активного аудиту є інформація про всі вразливості, ступені їх критичності і методи усунення, відомості про широкодоступну інформацію (інформація, доступна будь-якому потенційному порушнику) мережі замовника.

По закінченню активного аудиту видаються рекомендації з модернізації системи мережевого захисту, які дозволяють усунути небезпечні уразливості і тим самим підвищити рівень захищеності інформаційної системи від дій «зовнішнього» зловмисника при мінімальних витратах на інформаційну безпеку.

Однак без проведення інших видів аудиту ці рекомендації можуть виявитися недостатніми для створення «ідеальної» системи мережевого захисту. Наприклад, за результатами даного виду аудиту неможливо зробити висновок про коректність, з точки зору безпеки, проєкту інформаційної системи.

Активний аудит – послуга, яка може і повинна замовлятися періодично. Виконання активного аудиту, наприклад, раз на рік, дозволяє упевнитися, що рівень системи мережевого аудиту умовно можна розділити на два види - «зовнішній» і «внутрішній».

При «зовнішньому» активному аудиті фахівці моделюють дії «зовнішнього» зловмисника. У даному випадку проводяться такі процедури:

– визначення доступних із зовнішніх мереж ір-адрес замовника;

- сканування даних адрес з метою визначення працюючих сервісів і служб, а також призначення відсканованих хостів;
- визначення версій сервісів і служб сканованих хостів;
- вивчення маршрутів проходження трафіку до хостів замовника;
- збір інформації про замовника з відкритих джерел;
- аналіз отриманих даних з метою виявлення вразливостей.

«Внутрішній» активний аудит за складом робіт аналогічний «зовнішньому», проте при його проведенні за допомогою спеціальних програмних засобів моделюються дії «внутрішнього» зловмисника.

Цей поділ активного аудиту на «зовнішній» і «внутрішній» актуально для замовника в наступних випадках:

- у замовника існують фінансові обмеження в придбанні послуг і продуктів із захисту інформації;
- модель зловмисника, яку розглядає замовник, не включає «внутрішніх» зловмисників;
- в компанії замовника розслідується факт обходу системи мережевого захисту.

Призначення активного аудиту - виявляти і реагувати. Як зазначалося на початку, виявленню підлягає підозріла активність компонентів інформаційної системи (ІС) - від користувачів (внутрішніх і зовнішніх) до програмних систем і апаратних пристроїв.

Підозрілу активність можна поділити на зловмисну і аномальну (нетипову). *Зловмисна активність* - це або атаки, які мають на меті несанкціоноване отримання привілеїв, або дії, що виконуються в рамках наявних привілеїв (можливо, отриманих незаконно), але порушують політику безпеки. Останнє ми будемо називати зловживанням повноваженнями. Нетипова активність може прямо не порушувати політику безпеки, але, як правило, вона є наслідком або некоректної (або свідомо зміненої) роботи апаратури або програм, або дій зловмисників, що маскуються під легальних користувачів.

Активний аудит доповнює такі традиційні захисні механізми, як ідентифікація/автентифікація і розмежування доступу. Подібне доповнення необхідно з двох причин. По-перше, існуючі засоби розмежування доступу не здатні реалізувати всі вимоги політики безпеки, якщо останні мають більш складний вид, ніж дозвіл/заборона атомарних операцій з ресурсами. Розвинена політика безпеки може накладати обмеження на сумарний обсяг прочитаної інформації, забороняти доступ до ресурсу В, якщо раніше мав місце доступ до ресурсу А, і т.п. По-друге, в самих захисних засобах є помилки і слабкості, тому, крім будівництва огорож, доводиться дбати про відлов тих, хто зміг через ці паркани перелізти.

Розвинені системи активного аудиту несуть подвійне навантаження, утворюючи як перший, так і останній захисні рубежі (рис. 1.1). Перший рубіж призначений для виявлення атак і їх оперативного заходу. На останньому рубежі виявляються симптоми, які відбуваються в даний момент або раніше трапилися щодо порушення політики безпеки, вживаються заходи щодо припинення порушень і мінімізації збитку.

І на першому, і на останньому рубежі, крім активного аудиту, присутні інші сервіси безпеки. До першого рубежу можна віднести сканери безпеки, що допомагають виявляти й усувати слабкі місця в захисті. На останньому рубежі для виявлення симптомів порушень можуть використовуватися засоби контролю цілісності. Іноді їх включають в репертуар систем активного аудиту; ми, однак, не будемо цього робити, вважаючи контроль цілісності окремим сервісом.

Між сервісами безпеки існують і інші зв'язки. Так, активний аудит може спиратися на традиційні механізми протоколювання. У свою чергу, після виявлення порушення найчастіше потрібен перегляд раніше накопиченої реєстраційної інформації, оцінити збиток, зрозуміти, чому порушення стало можливим, спланувати заходи, що виключають повторення інциденту. Паралельно проводиться надійне відновлення первісної (тобто не зміненої порушником) конфігурації.

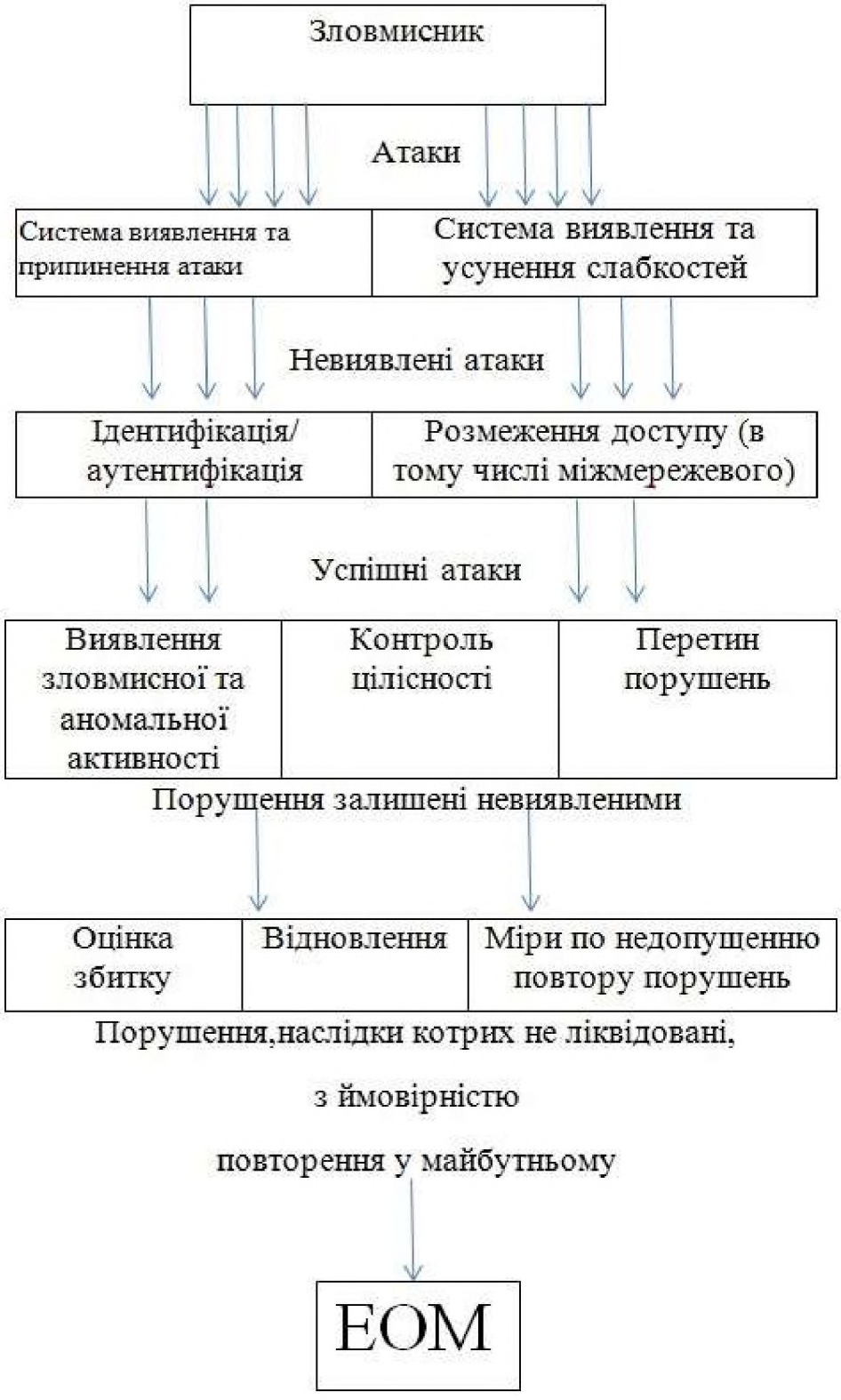

Рис. 1.1–Захисні рубежі, контрольовані системами активного аудиту

Окремим питанням є взаємодія систем активного аудиту та управління. Активний аудит виконує типові керуючі функції - аналіз даних про активність в інформаційній системі, відображення поточної ситуації,

автоматичне реагування на підозрілу активність. Подібним чином функціонує, наприклад, підсистема мережевого управління. На наш погляд, доцільно інтегрувати активний аудит і "загальне" управління, в максимально можливій мірі використовуючи загальні програмно-технічні та організаційні рішення. У цю інтегровану систему може бути включений і контроль цілісності, а також агенти іншої спрямованості, які відстежують специфічні аспекти поведінки ІС (рис. 1.2).

Рис. 1.2–Інтеграція сервісів безпеки і системи управління

З логічної точки зору можна вважати, що існує центральна консоль управління, куди стікаються дані від систем активного аудиту, контролю цілісності, аналізу захищеності, контролю систем і мереж по іншим аспектам. На цій консолі в тому чи іншому вигляді відображається поточна ситуація, з неї, автоматично або вручну, видаються керуючі команди. В силу технічних або організаційних причин ця консоль фізично може бути реалізована у вигляді декількох робочих місць (з виділенням, наприклад, місця адміністратора безпеки), але суть справи від цього не змінюється.

До зближення управління і сервісів безпеки рухаються обидві сторони. Так, в продукті компанії Computer Associates CA-Unicenter є потужна

підсистема управління безпекою, а новітня розробка - нейроагенти - використовує методи, типові при виявленні підозрілої активності.

З іншого боку, один з найвідоміших фахівців у галузі інформаційної безпеки Маркус Ранум (Markus Ranum) закликає "безпечників" відмовитися від трактування їх дисципліни як чогось ізольованого від мережевого управління. "Виявлення помилок, вторгнень або відмов - все це аспекти єдиної проблеми управління мережами" - зазначає він.

Сам Ранум слідує власним рекомендаціям, розглядаючи продукт для активного аудиту NFR (Network Flight Recorder) як компонент системи мережевого управління з відповідною реалізацією.

У наступних розділах ми ще не раз будемо зачіпати архітектурні питання, без вирішення яких неможливо створити результативну, гнучку, масштабовану систему активного аудиту.

1.2.1 Архітектура систем активного аудиту

У системі активного аудиту доцільно розрізняти локальну і глобальну архітектуру. В рамках локальної архітектури реалізуються елементарні складові, які потім можуть бути об'єднані для обслуговування корпоративних систем.

Основні елементи локальної архітектури та зв'язки між ними показані на рис. 1.3 Первинний збір даних здійснюють агенти, звані також сенсорами. Реєстраційна інформація може вилучатись з системних або прикладних журналів (технічно нескладно отримувати її і безпосередньо від ядра ОС), або добуватися з мережі за допомогою відповідних механізмів активного мережного обладнання або шляхом перехоплення пакетів допомогою встановленої в режим моніторингу мережевої карти.

На рівні агентів (сенсорів) може виконуватися фільтрація даних з метою зменшення їх обсягу. Це вимагає від агентів деякого інтелекту, але зате розвантажує інші компоненти системи.

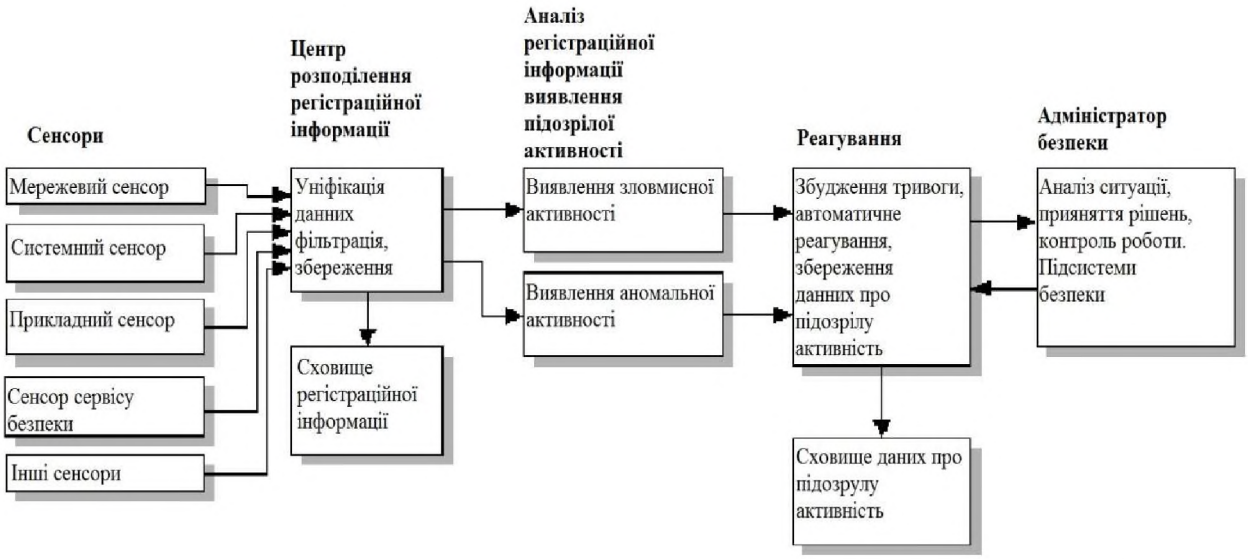

Рис. 1.3–Основні елементи локальної архітектури систем активного аудиту

Агенти передають інформацію в центр розподілу, який приводить її до єдиного (стандартному для конкретної системи активного аудиту) формату, можливо, здійснює подальшу фільтрацію (редукцію), зберігає в базі даних і направляє для аналізу статистичному і експертному компонентам. Один центр розподілу може обслуговувати декілька сенсорів.

Змістовний активний аудит починається зі статистичного і експертного компонентів (наприклад, тому, що для однохостових систем реєстраційну інформацію не треба якимось особливим чином витягувати і передавати). Ми детально розглянемо їх далі.

Якщо в процесі статистичного або експертного аналізу виявляється підозріла активність, відповідне повідомлення направляється вирішувачу, який визначає, чи є тривога виправданою, і вибирає спосіб реагування.

Зазвичай, коли пишуть про способи реагування, перераховують відправку повідомлення на телефон адміністратора, відправлення електронного листа йому ж тощо, тобто мають на увазі "ручне" вжиття заходів після отримання сигналу про підозрілу активність. На жаль, багато сучасних атак тривають секунди або навіть частки секунди, тому включення в процес реагування людини вносить неприпустимо велику затримку. Відповідні

заходи повинні бути в максимально можливій мірі автоматизовані, інакше активність аудиту багато в чому втрачає сенс.

Автоматизація потрібна ще й з тієї простої причини, що далеко не у всіх організаціях системні адміністратори володіють достатньою кваліфікацією для адекватного реагування на інциденти. Хороша система активного аудиту повинна вміти чітко пояснити, чому вона підняла тривогу, наскільки серйозна ситуація і які рекомендовані способи дії. Якщо вибір повинен залишатися за людиною, то нехай він зводиться до кількох елементів меню, а не до вирішення концептуальних проблем.

Ми залишаємо поза рамками нашого розгляду інтерфейси з СУБД (для зберігання і обробки реєстраційної інформації), і з системами управління, оскільки це стандартні технічні моменти, багаторазово описані в літературі. Ще раз підкреслимо, що безпека - це інфраструктурна властивість інформаційних систем. Сервіси безпеки повинні бути інтегровані з іншими інфраструктурними механізмами (управління, зберігання тощо), інакше експлуатація та розвиток інформаційної системи виявляться вкрай складними і дорогими.

Глобальна архітектура має на увазі організацію тимчасових і різнорангових зв'язків між локальними системами активного аудиту (рис. 1.4). На одному рівні ієрархії розташовуються компоненти, що аналізують підозрілу активність з різних точок зору. Наприклад, на хості можуть розташовуватися підсистеми аналізу поведінки користувачів і додатків. Їх може доповнювати підсистема аналізу мережевої активності. Коли один компонент виявляє щось підозріле, то в багатьох випадках доцільно повідомити про це сусідам або для вжиття заходів, або для посилення уваги до певних аспектів поведінки системи.

Різнорангові зв'язки використовуються для узагальнення результатів аналізу та отримання цілісної картини того, що відбувається. Іноді у локального компонента недостатньо підстав для порушення тривоги, але "за

сукупністю" підозрілі ситуації можуть бути об'єднані і спільно проаналізовані, після чого поріг підозрілості виявиться перевищеним.

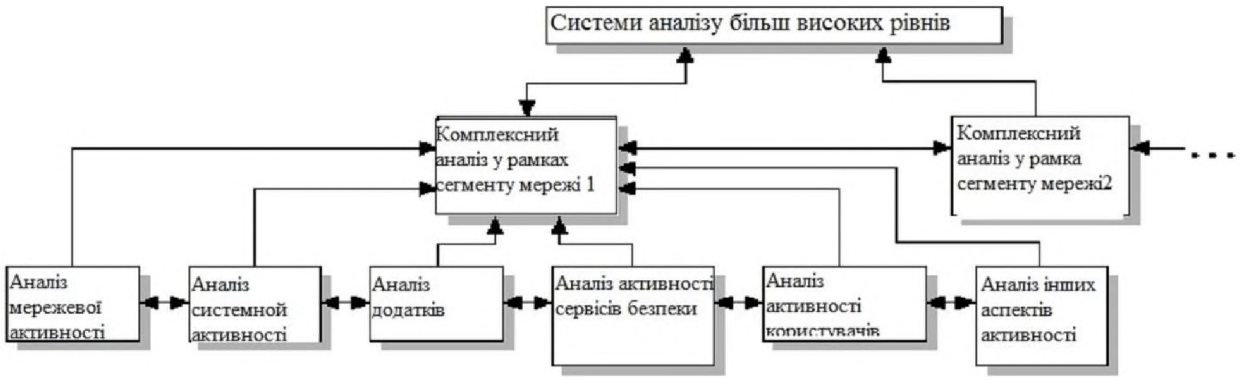

Рис 1.4– Глобальна архітектура системи активного аудиту

Цілісна картина, можливо, дозволить виявити скоординовані атаки на різні ділянки інформаційної системи і оцінити збиток в масштабі організації.

Очевидно, формування ієрархії компонентів активного аудиту необхідно і для вирішення проблем масштабованості, але цей аспект є стандартним для систем управління і ми не будемо на ньому зупинятися.

До числа найважливіших архітектурних відноситься питання про те, яку інформацію і в яких масштабах збирати та аналізувати. Перші системи активного аудиту були однохостовими. Потім з'явилися многохостові конфігурації. Прориву в області комерційних продуктів ми зобов'язані мережевим системам, які аналізували виключно мережеві пакети. Нарешті, в даний час, як і слід було очікувати, можна спостерігати конвергенцію архітектур, в результаті чого народжуються комплексні системи, які відстежують і аналізують як комп'ютерну, так і мережеву реєстраційну інформацію .

З багатьох причин корисно уявляти собі інформаційну систему як сукупність сервісів (а не мереж і вузлів). Відповідно, потрібно протоколювати і аналізувати поведінку сервісів незалежно від місця їх локалізації і ступеня розподіленості. Мережа, як така, забезпечує передачу даних (ми не беремо зараз в розрахунок додаткові мережеві сервіси, це окреме питання). Намагатися витягти з мережевого трафіку щось більше (наприклад,

інформацію про поведінку додатків) недоцільно, та й неможливо (ми повернемося до цього питання в розділі, присвяченому тестуванню систем активного аудиту). Навіть у такому просунутому продукті, як FireWall-1 компанії CheckPoint, не вдалося досягти повного успіху в справі фільтрації з відновленням контексту - розмежування міжмережевого доступу з точністю до команд прикладних протоколів залишилося можливим тільки при застосуванні "чесних" proxy-сервісів. Але ж у міжмережевих екранів мети аналізу простіші, ніж у систем активного аудиту.

Відомо, що без розуміння семантики захищаємих або аналізованих об'єктів забезпечення безпеки неможливо. Це розуміння може бути виражене в процедурному (програми) або декларативному (описи) видах, але воно повинно існувати. Декларативна семантика краще, оскільки вона дозволяє без змін застосовувати програмний продукт до різних об'єктів. Тут знову-таки напрошується аналогія з системами управління та адміністративними інформаційними базами (MIB).

Сучасні інформаційні системи в цілому не готові до ефективного управління. І ще більшою мірою цей висновок застосовний до активного аудиту. Програмні системи є "неаудируємі", немає ясних критеріїв, що дозволяють відрізнити нормальну поведінку від злочинного або аномального. У таких умовах наївно було б очікувати, що встановлені "поверх" кошти виявлення підозрілої активності створять диво і відіб'ють всі атаки. Втім, питання "аудируємих" програмних продуктів поки зовсім не досліджене, і ми не будемо на ньому зупинятися.

Традиційним є питання, де розміщувати сенсори систем активного аудиту. Настільки ж традиційна відповідь говорить: "скрізь, де можна". Тільки аналіз усіх доступних джерел інформації дозволить з достовірністю виявляти атаки та зловживання повноваженнями і докопуватися до їх першопричин. Якщо повернутися до трактування інформаційної системи у вигляді сукупності сервісів, то засоби виявлення атак повинні розташовуватися перед захищеними ресурсами (маючи на увазі напрямок руху

запитів до сервісів), а кошти виявлення зловживань повноваженнями - на самих сервісах. Виявлення аномальної активності корисно у всіх згаданих точках. Тільки при такому розміщенні сенсорів буде виконаний найважливіший принцип неможливості обходу захисних засобів. Крім того, буде мінімізовано число сенсорів, що в умовах сегментації мереж і застосування комутаційних технологій також виявляється проблемою.

До числа поширених відноситься і питання про те, як поєднувати засоби активного аудиту (в першу чергу, мережевого) і міжмережеві екрани. Зрозуміло, ці механізми безпеки не виключають, а доповнюють один одного. Наприклад, міжмережевий екран безсилий проти нелегальних модемних входів/виходів, а активний аудит дозволяє виявляти їх. Ще одне питання - розташовувати кошти виявлення атак перед фаєрволом, щоб захистити його. Цікаво, що за "круглим столом" фахівці висловлювали із цього приводу прямо протилежні думки. На наш погляд, міжмережевим екранам потрібно довіряти, вони є продуктом більш зрілої технології, ніж комерційні системи активного аудиту. Звичайно, доцільно контролювати цілісність конфігурації екрану, виявляти інші можливі аномалії, але це відбувається вже не зовні, а всередині. Якщо ж стає відомо про будь-які слабкості в програмному забезпеченні брандмауера, то їх, безсумнівно, потрібно негайно усувати, а не спостерігати за тим, як їх намагаються використати.

Для того, щоб система активного аудиту, особливо розподілена, була практично корисною, необхідно забезпечити цілісність аналізованої і переданої інформації, а також цілісність самої програмної системи і її живучість в умовах відмови або компрометації окремих компонентів (найчастіше атака направляється спочатку на засоби безпеки, а вже потім - на прикладні компоненти). Ясно, що це проблема всіх розподілених систем, і для її вирішення служать сервіси взаємної автентифікації і контролю цілісності (у тому числі перевірка автентичності джерела даних). На жаль, ситуація ускладнюється, якщо частина компонентів виявляється в неконтрольованій

зоні (наприклад, сенсори в віддаленій філії). Про це сказано у роботі з комп'ютерної імунології [12] , живучості розподілених систем [13] і книзі [14] , в якій у фарбах описується застосування впливу на сенсори в якості потужної зброї.

1.2.2 Виявлення зловмисної активності

Під зловмисною активністю ми розуміємо як атаки (очевидно, що суперечать будь-якій політиці безпеки), так і дії, що порушують політику безпеки конкретної організації шляхом зловживання наявними повноваженнями. Поділ двох видів зловмисної активності представляється нам доцільним з тієї причини, що налаштування на виявлення атак може бути виконане постачальником системи активного аудиту (атаки носять універсальний характер), у той час як політика безпеки (якщо, звичайно, вона є) у кожної організації своя і налаштовуватися на неї замовникам доведеться самим.

Для виявлення зловмисної активності намагалися і намагаються використовувати декілька універсальних технологій: експертні системи, нейронні мережі, зіставлення зі зразком, кінцеві автомати і т.п. Однією з перших і до цих пір самої вживаною залишається технологія виявлення сигнатур зловмисних дій. Ідея полягає в тому, щоб якимось чином задати характеристики злочинного поведінки (це і називається сигнатурами), а потім відстежувати потік подій в пошуках відповідності з зумовленими зразками. Іноді зіставлення ґрунтується на простому (стосовно активного аудиту - наївному) механізмі регулярних виразів, відомому всім по ОС Unix. У більш серйозних розробках вже понад десять років використовуються експертні системи, що спираються на набори правил, що
задають більш потужні мови.

Грубо можна вважати, що експертна система складається з універсальної оболонки та наповнення у вигляді правил виводу, що є формалізацією знань про предметну область. В області активного аудиту найчастіше

використовується оболонка P-BEST (Production-Based Expert System Toolset). Її і розглянемо разом з деякими сигнатурами атак, запозиченими з тієї ж статті [15] .

Важливо, питання ефективності і сполучення з оточенням (зазвичай керуючим) P-BEST відноситься до категорії систем прямого зв'язування, тобто вона відправляється від відомих фактів, зіставляє їх із записаними в правилах умовами і виводить нові факти до тих пір, поки не буде досягнута мета (у нашому випадку - виявлена зловмисна активність).

Кожне правило складається з двох частин: умови застосовності (званого також антецедентом) і правій частині - консеквента. Коли чергова подія в відстежуємому потоці робить істинним умову застосовності деякого правила, кажуть, що правило "запалюється". Якщо наслідок містить будь-які дії, вони виконуються (або поміщаються в поле зору компонента, що приймає рішення про реагування на зловмисну активність).

До складу P-BEST входить компілятор pbcc, що транслює правила виведення в функції мови С. Після компіляції може бути отримана або самостійна експертна система, або набір бібліотек, які можна підключити до більш широкого оточення. Для нас важливо, що мова P-BEST досить проста і інтуїтивно зрозуміла, тому в принципі користувачі самі можуть описувати на ньому нові атаки і інші зловмисні дії. Компіляція (на противагу інтерпретації) правил дозволяє отримати ефективне рішення, придатне для роботи в реальному масштабі часу. До складу антецедентів і консеквента можуть входити довільні функції мови С. Це спрощує зв'язок з оточенням, програмування реакцій і т.п.

Наведемо приклад простого правила, записаного на мові P-BEST . Воно обробляє невдалу спробу входу в систему. Передбачається, що раніше були описані типи event і bad_login з відповідними полями.

Лістинг 1

```
rule [Bad_Login (# 10; *): [e: event | event_type == login, return_code ==
```

'BAD_PASSWORD] ==> [+ bad_login | username = e.username, hostname - e.hostname] [- | e] [! | printf ("Bad login for user% s from host% s \ n", e.username, e.hostname)]]

У першому рядку, крім назви правила, вказано його пріоритет (10), що впливає на порядок виконання, а також дано дозвіл на його багаторазове застосування. Щоб не сталося зациклення, оператор "[- | e]" в консеквента видаляє факт e з бази фактів, але попередньо в цю базу додає факт bad_login, який потім можна використовувати, наприклад, для підрахунку числа невдалих спроб входу. Нарешті, конструкція "! |" Дозволяє виконувати функції мови C. Зрозуміло, в реальних системах реакція повинна бути більш витонченою.

В якості реального прикладу використання мови P-BEST розглянемо правило, ідентифікуюче атаки за допомогою переповнення буфера, зарезервованого для зберігання параметрів (Лістинг 2). Подібні атаки використовують помилки в програмному забезпеченні, пов'язані з перевіркою коректності параметрів (точніше, з відсутністю або недостатністю таких перевірок). Якщо відповідним чином задати занадто довгі параметри деяким утилітам, що виконуються від імені суперкористувача (таким, наприклад, як eject або fdformat в Solaris 2.5), можна виконати в привілейованому режимі довільну команду.

Наведене нижче правило розраховане на модуль реєстрації / аудиту BSM в ОС Solaris. Ідея виявлення атак за допомогою переповнення буфера заснована на аналізі довжини аргументів системних викликів групи exec. Виявляється, розмір облікової записи про "образами" exec становить не менше 500 байт, в той час як в нормальних випадках він практично ніколи не перевищує 400.

Лістинг 2

```
rule [BSM_LONG_SUID_EXEC (*): [+ e: bsm_event] [? | e.header_event_type == AUE_EXEC || e.header_event_type == AUE_EXECVE] [? | e.subject.euid! = e.subject.ruid] [? | e.header_size> 'NORMAL_LENGTH] ==> [! | printf ("ALERT: buffer overrun attack on command% s \ n", e.header_command)]]
```

Наприклад, набір для виявлення атак на доступність "SYN flood" складається з семи правил, найдовше з яких налічує 12 рядків. Це означає, що подібні набори цілком реально розробляти самостійно.

Втім, виразна сила мови правил для експертних систем ніколи не викликала сумнівів. Традиційною проблемою була ефективність функціонування. Згідно з наведеними даними, на обробку реєстраційного журналу розміром 1.41 ГБ з числом записів 4.2 мільйона при 16 наборах правил на комп'ютері з процесором Pentium II (330 МГц) і операційною системою FreeBSD 2.2.6 знадобилося трохи більше 30 хвилин. Журнал був накопичений за п'ять діб (120 годин) роботи. Значить, пошук сигнатур в даному випадку забирає менше 0.5% процесорного часу. Оскільки, як з'ясувалося, час обробки зростає значно повільніше, ніж перша ступінь числа правил, є маса резервів для збільшення кількості сигнатур і ускладнення виконуваних перевірок.

Таким чином, підхід, заснований на виявленні сигнатур зловмисних дій засобами експертних систем, виявляється цілком працездатним з усіх точок зору.

Підкреслимо ще раз, що виразна сила мови регулярних виразів для завдання сигнатур, звичайно, не є достатньою в силу можливості варіацій при проведенні атак. Проста фрагментація IP-пакетів або зміна значень, що маємо на увазі, в злобливому коді на якісь інші (наприклад, зміна вхідного імені та / або пароля відомої програми Back Orifice здатна обдурити систему активного аудиту, що використовує жорсткі сигнатури. Системи на основі регулярних

виразів робити відносно нескладно, але технологічно вони вже застаріли, незалежно від займаної ними частки ринку.

Втім, справедливості заради слід зазначити, що проблема стійкості сигнатур по відношенню до варіацій зловмисних дій в більшій чи меншій мірі неприємна для будь-якого підходу.

Але найскладнішою проблемою для сигнатурного підходу є виявлення раніше невідомих атак. Вище ми вказували, що нові загрози з'являються практично щодня. Боротися з ними можна двома способами.

По-перше, можна регулярно оновлювати набір сигнатур. Тут, крім повноти, критично важливою є частота оновлень. Сигнатури нових атак повинні надаватися замовникам на порядок швидше, ніж латки від виробників скомпрометованих апаратних або програмних продуктів. На практиці це означає оновлення протягом доби, але ніяк не раз на місяць. В іншому випадку системи активного аудиту починають нагадувати фіговий листок, а не засіб захисту від реальних загроз.

По-друге, можна (і потрібно) поєднувати сигнатурний підхід з методами виявлення аномальної активності, до розгляду яких й переходимо. Атака або зловживання повноваженнями - це майже завжди аномалія. Справа за малим - не пропустити її і не піднімати занадто часто помилкових тривог.

1.2.3 Виявлення аномальної активності

Для виявлення аномальної активності було запропоновано досить багато методів [17] : нейронні мережі, експертні системи, статистичний підхід. У свою чергу, статистичний підхід можна поділити на кластерний і факторний аналіз, а також дискримінантний (класифікаційний) аналіз. Не вдаючись у деталі, зазначимо, що буквальне застосування цих методів не дає хороших результатів; необхідно враховувати специфіку предметної області - активного аудиту.

Статистичний аналіз (з урахуванням зроблених застережень) представляється нам найбільш перспективним, почасти "від протилежного",

в силу недоліків, властивих іншим підходам.

У нейронних мережах дві основні проблеми:

– незрозумілість результатів: нейронна мережа приймає рішення, але не пояснює, чому воно було прийнято;
– нестача адекватного навчального матеріалу: неможливо створити базу всіх типів аномалій.

Публікації з анонсами "майже працюючих" нейронних мереж з'являлися неодноразово, однак не доводилося читати про готові і працюючі системи.

Основний недолік експертних систем був вказаний вище - невміння виявляти (і, отже, відображати) невідомі атаки.

– У статистичного підходу також є проблеми:
– відносно висока ймовірність помилкових тривог (нетиповість поведінки не завжди означає злий умисел);
– погана робота у випадках, коли дії користувачів не мають певного шаблону, коли з самого початку користувачі здійснюють злочинні дії (злочинні дії типові), нарешті, коли користувач поступово змінює шаблон своєї поведінки в бік злочинних дій.

Проте, як показує досвід, з цими проблемами можна боротися.

Виявлення аномальної активності статистичними методами ґрунтується на порівнянні короткострокової поведінки з довгостроковою. Для цього вимірюються значення деяких параметрів роботи суб'єктів (користувачів, додатків, апаратури). Параметри можуть відрізнятися за своєю природою; можна виділити наступні групи:

– категоріальні (змінені файли, виконані команди, номер порту і т.п.);
– числові (процесорний час, обсяг пам'яті, кількість переглянутих файлів, число переданих байт тощо);
– величини інтенсивності (число подій в одиницю часу);
– розподіл подій (таких як доступ до файлів, виведення на друк і т.п.).

Алгоритми аналізу можуть працювати з різнорідними значеннями, а можуть перетворити всі параметри до одного типу (наприклад, розбивши область значення на кінцеве число підобластей і розглядаючи всі параметри як категоріальні). Вибір вимірюваних характеристик роботи - дуже важливий момент. З одного боку, недостатнє число фіксованих параметрів може привести до неповноти опису поведінки суб'єкта і до великого числа пропуску атак; з іншого боку, занадто велике число відслідковуються характеристик потребують занадто великого обсягу пам'яті і сповільнить роботу алгоритму аналізу. Вимірювання параметрів накопичуються і перетворюються в профілі - опису роботи суб'єктів. Суть перетворення безлічі результатів вимірювання в профілі - стиснення інформації. В результаті від кожного параметра має залишитися лише кілька значень статистичних функцій, що містять необхідні для аналізу алгоритму дані. Для того, щоб профілі адекватно описували поведінку суб'єкта, необхідно відкидати старі значення параметрів при перерахунку значень статистичних функцій. Для цього, як правило, використовується один з двох методів:

- метод ковзких вікон - результати вимірювань за деякий проміжок часу (для довгострокових профілів - кілька тижнів, для короткострокових - кілька годин) зберігаються; при додаванні нових результатів старі відкидаються. основним недоліком методу ковзних вікон є великий об'єм інформації.
- метод зважених сум - при обчисленні значень статистичних функцій більш старі дані входять з меншими вагами (як правило, нові значення функцій обчислюються за рекурентною формулою, і необхідність зберігання великої кількості інформації відпадає). Основним недоліком методу є більш низька якість опису поведінки суб'єкта, ніж у методі ковзних вікон.

Отже, довгострокові профілі містять у собі інформацію про поведінку суб'єктів за останні кілька тижнів; зазвичай вони перераховуються раз на добу, коли завантаження системи мінімальне. Короткострокові профілі містять

інформацію про поведінку за останні кілька годин або навіть хвилин; вони перераховуються при надходженні нових результатів вимірювань.

Порівняння короткострокових і довгострокових профілів може проводитися різними способами. Можна просто перевіряти, чи короткострокові значення потрапляють в довірчі інтервали, побудовані за довгостроковим профілем. Однак у цьому випадку аномалії, розподілені за кількома параметрами, можуть залишитися непоміченими. Тому краще аналізувати профілі в сукупності. Далі, вимірювані характеристики, як правило, не є незалежними, тому було б бажаним, щоб вплив параметрів на рішення про типовість поведінки було пропорційно ступеню їх незалежності.

У роботі [18] розглядається ряд сценаріїв мережевої активності і пропонуються ефективно працюючі набори параметрів. Так, для сервісів типу SMTP або FTP доцільно відстежувати категоріальні характеристики: імена каталогів, до яких здійснюється доступ; протоколи, що використовуються для певних портів; типи фіксуються помилок.

Відзначимо, що корисною числовою характеристикою є кількість зафіксованих помилок. При цьому виявляється не тільки зловмисну поведінку, а й збої і відмови апаратури і програм, що також можна вважати порушенням інформаційної безпеки. Зрозуміло, доцільно вимірювати і обсяг мережевого трафіку. Аномальними є відхилення в обидві сторони (занадто великий трафік - сервіс використовують в злочинних цілях, занадто маленький - порушена доступність сервісу).

Стосовно мережевого трафіку і деяким іншим подіям, корисним класом величин виявляється інтенсивність. Наприклад, різке наростання спроб встановлення транспортних сполучень може бути свідченням SYN-атаки або сканування портів.

Аналіз розподілу подій дозволяє встановити, як події, що впливають на ті чи інші значення. Наприклад, виконання команди cd в FTP-сеансі впливає на категоріальну величину "каталоги", але не впливає на величини, асоційовані з файлами. Якщо трапилося зворотне, значить, нормальна робота

FTP-сервісу з яких-небудь причин порушена. Взагалі аналіз розподілу подій - ефективний спосіб виявлення кореляцій, зокрема, між сигналами, які надходять на центральну консоль від підсистем активного аудиту. Можливо, з точки зору окремих підсистем події виглядають не настільки підозрілими, щоб піднімати тривогу, але спільний аналіз розподілів дозволяє виявити скоординовану атаку.

Для успіху статистичного підходу важливий правильний вибір суб'єктів, поведінка яких аналізується. На наш погляд, доцільно аналізувати поведінки сервісів або їх компонентів (наприклад, доступ анонімних користувачів до FTP-сервісу). У порівнянні з окремими користувачами, поведінка сервісів відрізняється більшою стабільністю, та й для інформаційної безпеки організації важливі саме сервіси. Зовсім немає сенсу аналізувати мережевий трафік "взагалі", його також потрібно структурувати за типами підтримуваних сервісів (плюс службові моменти мережевого і транспортного рівнів, такі як встановлення з'єднань).

Статистичний підхід є предметом інтенсивних досліджень, але вже зараз він володіє достатньою зрілістю, використовується в академічних та комерційних розробках. Можна очікувати, що з часом його позиції будуть зміцнюватися. У всякому разі, системи активного аудиту, в яких статистичний компонент відсутній, не можуть претендувати на повноту захисних функцій.

1.2.4 Реагування на підозрілі дії

Після того, як виявлена сигнатура злочинної дії або нетипова активність, необхідно вибрати гідну відповідь. З багатьох міркувань зручно, щоб компонент реагування містив власну логіку, фільтруючи сигнали тривоги і зіставляючи повідомлення, що надходять від підсистем аналізу. Для активного аудиту однаково небезпечні як пропуск атак (це означає, що не забезпечується належного захисту), так і велика кількість помилкових тривог (це означає, що активний аудит швидко відключать).

При виборі реакції особливо важливо визначити першопричину проблем. Для мережевих систем це особливо складно в силу можливості підробки адрес в пакетах. Цей приклад показує, що сильнодіючі засоби, які намагаються впливати на зловмисника, самі можуть стати непрямим способом проведення атак.

Перевага надається більш спокійним, але також досить ефективним заходам, такі як блокування зловмисного мережевого трафіку засобами міжмережевого екранування (ряд систем активного аудиту вміють керувати конфігурацією екранів) або примусове завершення сеансу роботи користувача. Звичайно, і тут залишається небезпека покарати невинного, так що політика безпеки кожної організації повинна визначати, що важливіше - не пропустити порушення або не образити лояльного користувача.

З точки зору швидкого реагування, традиційні заходи, пов'язані з інформуванням адміністратора, не дуже ефективні. Вони гарні в довгостроковому плані, для глобального аналізу захищеності командою професіоналів. Тут активний аудит змикається з пасивним, забезпечуючи стиск реєстраційної інформації і представлення її у вигляді, зручному для людини.

Розумна реакція на підозрілі дії може включати збільшення ступеня деталізації протоколів та активізацію засобів контролю цілісності. В принципі, це пасивні заходи, але вони допоможуть зрозуміти причини і хід розвитку порушення, так що людині буде простіше вибрати "запобіжний захід".

Ймовірно, в перспективі нормою стане взаємодія з системами, через які надходить підозрілий мережевий трафік. Це допоможе припиненню зловмисної активності і простежуванню порушника. Деякі підходи до даної проблеми більш детальніше розглянуто в наступному розділі "Вимоги до систем активного аудиту".

1.2.5 Вимоги до систем активного аудиту

У цьому пункті ми розглянемо вимоги до систем активного аудиту, істотні з точки зору замовників.

На перше місце слід поставити вимогу повноти. Це дуже ємне поняття, яке включає в себе наступні аспекти:

- Повнота відстеження інформаційних потоків до сервісів. Активний аудит повинен охоплювати всі потоки всіх сервісів. Це означає, що система активного аудиту повинна містити мережеві і системні сенсори, аналізувати інформацію на всіх рівнях від мережевого до прикладного. Очевидно, з розглянутого аспекту повноти випливає вимога розширюваності,ос кільки ні один програмний продукт НЕ може бути спочатку налашто ваний на всі сервіси.
- Повнота спектра виявлення атак і зловживань повноваженнями. Дана вимога означає не тільки те, що у системи повинен бути досить потужна мова опису підозрілої активності (як атак, так і зловживань повноваженнями). Ця мова має бути проста, щоб замовники могли робити настроювання системи у відповідності зі своєю політикою безпеки. Постачальник системи активного аудиту повинен в найкоротші терміни (порядку діб) передавати замовнику сигнатури нових атак. Система повинна вміти виявляти аномальну активність, щоб справлятися із заздалегідь невідомими способами порушень.
- Достатня продуктивність. Система активного аудиту повинна справлятися з піковими навантаженнями захищуваних сервісів.

Пропуск навіть одного мережевого пакету може дати зловмисникові шанс на успішну атаку. Якщо відомо, що система активного аудиту володіє недостатньою продуктивністю, вона може стати об'єктом атаки на доступність, на тлі якої будуть розвиватися інші види нападу. Для локальних мереж стандартними стали швидкості 100 Мбіт/с. Це вимагає від системи

активного аудиту дуже високої якості реалізації, потужної апаратної підтримки. Якщо врахувати, що захищаються сервіси знаходяться в постійному розвитку, то стане зрозуміло, що вимога продуктивності одночасно є і вимогою масштабованості.

Крім повноти, системи активного аудиту повинні відповідати таким вимогам:

- Мінімум помилкових тривог. В абсолютному вираженні допустимо не більше однієї помилкової тривоги на годину (краще, якщо їх буде ще на порядок менше). При інтенсивних потоках даних між сервісами і їх клієнтами подібна вимога виявляється вельми жорсткою. Нехай, наприклад, в секунду по контрольованому каналу проходить 1000 пакетів. За годину пакетів буде 3 600 000. Можна припустити, що майже всі вони НЕ є зловмисними. І тільки один раз система активного аудиту має право прийняти «свого» за «чужого», то ймовірність помилкової тривоги повинна складати в даному випадку НЕ більше $3 * 10^{-7}$.
- інтеграція з системою управління та іншими сервісами безпеки. інтеграція з системою управління має дві сторони. по-перше, самі засоби активного аудиту повинні управлятися (встановлюватися, конфігуруватися, контролюватися) нарівні з іншими інфраструктурними сервісами. по-друге, активний аудит може (і повинен) поставляти дані в загальну базу даних управління. інтеграція з сервісами безпеки необхідна як для кращого аналізу ситуації (наприклад, із залученням засобів контролю цілісності), так і для оперативного реагування на порушення (засобами додатків, операційних систем або міжмережевих екранів). наявність технічної можливості віддаленого моніторингу інформаційної системи. це спірна вимога, оскільки не всі організації захочуть опинитися під чиїмось "ковпаком". наприклад, в США плани адміністрації Клінтона з моніторингу інформаційних систем федеральних організацій натрапили на жорстку протидію.

Проте, з технічної точки зору, подібна міра цілком виправдана, оскільки більшість організацій не володіють кваліфікованими фахівцями з інформаційної безпеки.

Зазначимо, втім, що віддалений моніторинг може бути використаний і для безперечних цілей, таких як контроль з штаб-квартири за роботою віддалених відділень.

Сформульовані вимоги можна вважати максималістськими. Мабуть, жодна сучасна комерційна система, жоден постачальник не задовольняють їм повною мірою, однак, без їх виконання активний аудит перетворюється з серйозного оборонної зброї в сигналізацію для відлякування дітей молодшого шкільного віку. Часто замовники не згодні платити гроші за подібне. Але, звичайно, якщо тільки вони досить розбираються в предметі.

Системи активного аудиту належать до області високих технологій. У них розвинена математична база, просунута архітектура, вони увібрали в себе знання з інформаційної безпеки. Мало хто з реселерів розуміє, як працює те, що вони продають; їм залишається переказувати рекламні буклети виробників, де, звичайно, все виглядає чудово. Замовники теж не зобов'язані вдаватися в деталі, але вони повинні знати, про що питати постачальників. Не завжди ті зможуть відповісти, але і мовчання багато що скаже замовнику.

1.3 Тестування на проникнення (аудит інформаційної безпеки)

Аудит інформаційної безпеки (тест на проникнення) дозволяє Компанії отримати оцінку реального рівня захищеності інформаційних активів в умовах сучасного стану методів отримання несанкціонованого доступу до інформаційних активів, оброблюваних в автоматизованих інформаційних системах організацій. Отримання такої оцінки забезпечується шляхом моделювання атак потенційних зловмисників на обрані інформаційні активи Компанії.

Перелік інформаційних активів і вектори модельованих атак визначаються на початковому етапі проведення тесту на проникнення і узгоджуються з Компанією.

В якості цільових для потенційного зловмисника активів можуть виступати як внутрішня корпоративна мережа Компанії, так і конкретні інформаційні системи, в тому числі що містять критичні для Компанії дані.
Тест на проникнення дозволяє досить швидко оцінити реальну захищеність обраних інформаційних активів від несанкціонованого доступу, моделюючи найбільш поширені атаки.

Основною відмінною особливістю тесту на проникнення в порівнянні з традиційним аудитом інформаційної безпеки є:

- зазвичай менша глибина охоплення інформаційної інфраструктури організації;
- велика деталізація знайдених вразливостей;
- більш точна оцінка ризиків ІБ (ґрунтується на результатах реалізації знайдених вразливостей);
- більша вірогідність результатів аудиту (в порівнянні з класичними методами аудиту, заповнення анкет, опитування співробітників і т.д.);
- оцінка більшої кількості процесів ІБ, ніж при інструментальному аудиті, включаючи оцінку процесів (наприклад, управління інцидентами, моніторинг і т.д.), об'єктивна оцінка яких не може бути отримана іншими засобами (інструментальний аудит, анкетування і інтерв'ювання і т.д.);
- детальне опрацювання знайдених вразливостей, що дозволяє отримати більш об'єктивну оцінку процесів забезпечення інформаційної безпеки організації.

В даний час існує декілька міжнародних методик проведення тестування на проникнення, орієнтованих в основному на моделювання атак, спрямованих на мережеву інфраструктуру організації:

- open source security testing methodology manual (osstmm) – мабуть, єдина методика, яка акцентує увагу не тільки на технічних тестах, але і на атаках пов'язаних мережі;
- nist sp800-115 – документ, хоча і не є методикою, але описує загальні аспекти тестів на проникнення;
- the information systems security assessment framework (issaf) – фреймворк (framework), орієнтований на інструментальний пошук вразливостей;
- pci dss (розділ 11.3 стандарту) – згідно розділу 11.3. стандарту pci dss в організаціях, відповідних стандарту, не рідше 1 разу на рік повинен проводитися тест на проникнення. для роз'яснення даного розділу PCI DSS був випущений документ Information Supplement t 11.3 Penetration Testing, який в загальних рисах описує послідовність проведення інструментальної перевірки зовнішнього периметра мережевої інфраструктури компанії, що тестується (по суті, дана інструментальна перевірка не є тестом на проникнення);
- зазвичай при проведенні робіт, використовується власна методику проведення тестів на проникнення, що включає в себе можливість моделювання не тільки технічних атак на інформаційні ресурси доступні з мережі інтернет (широко застосовуваних у міжнародних методологіях OSSTMM, ISSAF і PCI DSS), але й атаки, направлені на користувачів корпоративних систем (соціальна інженерія), бездротові мережі IEEE 802.11 (Wi-Fi), 802.15 (Bluetooth) і 802.16 (Wi-Max), переносні комп'ютери та мобільні пристрої, а так само атаки з використанням фізичного або логічного доступу до компонентів корпоративної інформаційної системи.

Перелік модельованих атак може бути сформований на етапі підготовки технічного завдання і додатково скоректований у ході проведення тесту на проникнення.

При проведенні робіт можуть бути перевірені наступні вектори проведення атак приведені в таблиці 1.1

Таблиця 1.1 - Вектори проведення атак

№	Вектор атаки	Опис
1	Фізичний	Атаки з використанням безпосереднього фізичного доступу всередину захищається периметра корпоративної мережі (якщо такий є)
2	Мережевий	Дистанційні атаки на мережеві ресурси і протоколи
3	Електронна пошта	Атаки з використанням електронної пошти (у тому числі з елементами соціальної інженерії)
4	Додатки	Атаки з використанням специфічних додатків використовуваних Замовником (наприклад, web портал)
5	Бездротові мережі	Атаки напрямок на бездротові протоколи передачі даних 802.11 (Wi-Fi), 802.15 (Bluetooth), 802.16 (Wi-Max)
6	Клієнтські програми	Атаки на клієнтські програми
7	Мобільні пристрої	Атаки на мобільні пристрої (мобільні та переносні комп'ютери, смартфони і т.д.)
8	Соціальна інженерія	Атаки на користувачів з використанням методів соціальної інженерії

Також передбачається проведення тестування на проникнення. Тестування проводиться в один етап і складається з робіт, зазначених у таблиці 1.2

Таблиця 1.2 Роботи які проводяться при тестуванні

№	Перелік робіт	Звітні документи
1	Планування робіт	Технічне завдання на проведення тесту на проникнення
2	Проведення тесту на проникнення	Робочі матеріали
3	Аналіз результатів і підготовка підсумкового звіту	Звіт за результатами проведення аудиту інформаційної безпеки (тесту на проникнення)

За проведення тесту на проникнення розробляється звіт про тестування, який, як правило, містить:

- опис меж, в рамках яких було проведено тест на проникнення;
- методи і засоби, які використовувалися в процесі проведення тесту на проникнення;
- опис виявлених вразливостей і недоліків, включаючи рівень їх ризику і можливість їх використання зловмисником;
- опис застосованих сценаріїв проникнення;
- опис досягнутих результатів;
- базову оцінку ризиків інформаційної безпеки компанії;
- базову оцінку процесів забезпечення інформаційної безпеки компанії;
- рекомендації щодо усунення виявлених вразливостей і вдосконаленню процесів забезпечення інформаційної безпеки компанії;
- план робіт з усунення знайдених вразливостей і вдосконаленню процесів забезпечення інформаційної безпеки компанії, пріоритезувати відповідно до критичністю вразливостей.

Так само, для більш наочного подання результатів тестування, для керівництва Замовника може бути проведена презентація.

1.3.1 Процес тестування на проникнення

Тестування на проникнення (penetration testing) являє собою процес моделювання атак на мережі (рис. 1.8) та системи на прохання їх власника - керівника вищої ланки. При тестуванні на проникнення тестувальник використовує набір процедур та інструментів, призначених для тестування і спроб обходу захисних заходів системи. Метою тестування на проникнення є оцінка рівня опору компанії атаці і виявлення будь-яких недоліків в її середовищі. Компанії потрібно незалежно оцінити ефективність своїх заходів безпеки, а не просто довіритися обіцянкам постачальників. Хороша комп'ютерна безпека ґрунтується на реальних фактах, а не на одному тільки поданні, як все має працювати.

Тестування на проникнення імітує ті ж методи, які використовують реальні зловмисники. Потрібно враховувати, що зловмисники можуть бути дуже розумними, творчими людьми, вельми винахідливими у своїх підходах, тому тестування на проникнення повинно також використовувати новітні методи злому поряд з міцною методологією проведення такого тестування. У процесі тестування потрібно проаналізувати кожен комп'ютер в середовищі, як показано на малюнку 10-5, оскільки не варто розраховувати, що зловмисник просканує тільки один або два комп'ютера і, не знайшовши в них вразливостей, вибере іншу компанію.

Можливості сканерів вразливостей.

Сканери вразливостей надають такі можливості:

- виявлення активних систем в мережі;
- виявлення активних вразливих служб (портів) на знайдених системах;
- виявлення працюючих на них додатків і аналіз банерів;
- визначення встановлених на них операційних систем;
- виявлення вразливостей, пов'язаних з виявленими операційними системами і додатками;

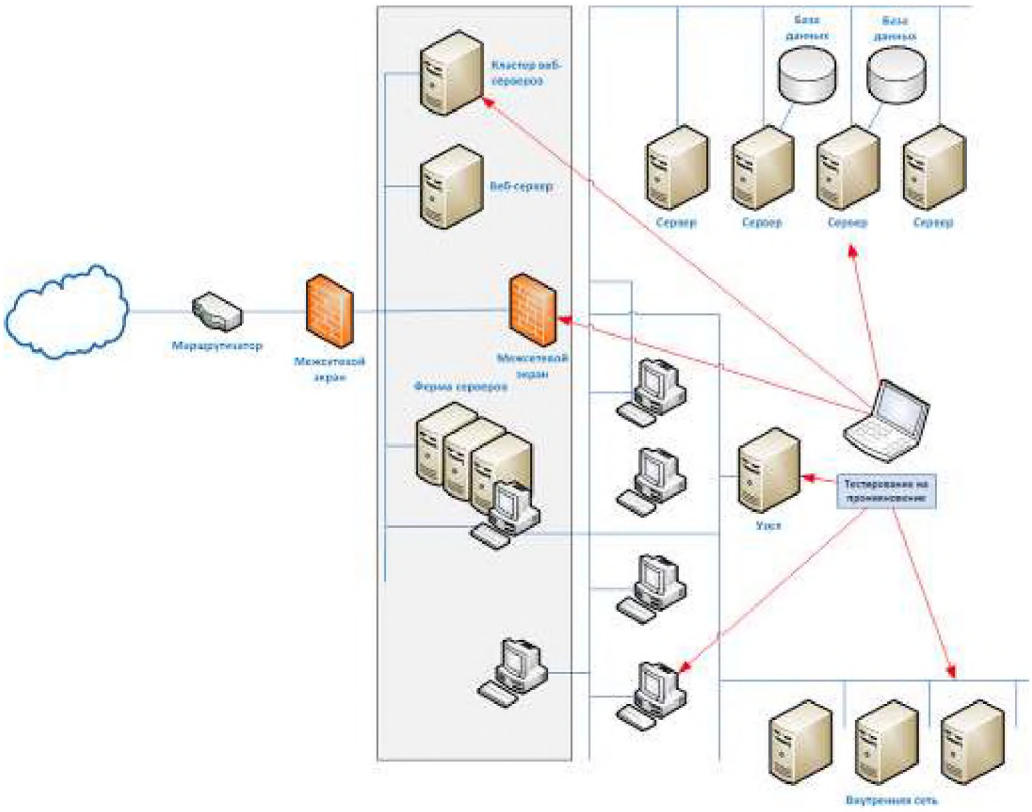

Рис. 1.8 – Схема мережевих зв'язків

– виявлення неправильних налаштувань;
– тестування на відповідність з політиками використання додатків і політикам безпеки;
– підготовка основи для проведення тестування на проникнення.

Вибір варіанту тестування на проникнення залежить від компанії, її цілей щодо безпеки і цілей її керівництва. Деякі великі компанії регулярно виконують тестування на проникнення в своє середовище, використовуючи різні види інструментів, або застосовуючи скануючі пристрої, які безперервно аналізують мережу компанії, автоматично виявляючи в ній нові уразливості. Інші компанії звертаються до постачальників відповідних послуг для виявлення вразливостей і проведення тестування на проникнення, щоб отримати більш об'єктивну думку про захищеність свого середовища.

При тестуванні на проникнення можуть бути перевірені веб-сервери, DNS -сервери, налаштування маршрутизаторів , проаналізовано уразливості робочих станцій, перевірена можливість доступу до критичної

інформації, перевірені системи віддаленого доступу, відкриті порти, властивості доступних служб і все інше, чим може скористатися реальний зловмисник, щоб отримати несанкціонований доступ до захищених інформаційних активів компанії. Деякі тести можуть чинити негативний вплив на роботу систем, виводити їх з ладу. Терміни проведення тестування повинні бути заздалегідь узгоджені. У процесі тестування не повинно чинитися істотного впливу на продуктивність роботи компанії, а персонал компанії повинен бути готовий при необхідності оперативно відновити роботу систем.

За результатами тестування на проникнення повинен бути оформлений звіт, що описує виявлені вразливості і ступінь їх критичності, а також рекомендації щодо їх виправлення. Цей звіт має бути наданий керівництву компанії. На підставі звіту керівництво має визначити, з чим насправді пов'язані виявлені вразливості, і наскільки ефективні реалізовані контрзаходи. Вкрай важливо, щоб керівники вищого рівня добре розуміли ризики, пов'язані з проведенням тестування на проникнення - відповідна інформація має бути надана їм перед тим, як вони дадуть свій дозвіл на проведення тестування. Це пов'язано з тим, що в окремих випадках використовуються інструменти та методики тестування на проникнення можуть вивести з ладу системи або програми. Метою тестування на проникнення є пошук вразливостей, оцінка реальної ефективності використовуваних компанією заходів і засобів безпеки, аналіз реагування систем і персоналу безпеки на підозрілу активність, аналіз видаваних системами попереджень (які можуть і не з'явитися).

Фахівці з безпеки перед проведенням тестування на проникнення повинні отримати офіційний документ (лист) від керівництва компанії, в якому вказані, зокрема, дозволені межі тестування. Цей документ повинен бути доступний всім членам команди, які беруть участь у процесі проведення тестування. Цей документ часто називають «перепусткою на вихід з в'язниці» (Get Out of Jail Free Card). Крім того, учасникам тестування повинна бути доступна контактна інформація ключового персоналу компанії, і «дерево

викликів» на випадок, якщо щось піде не за планом, і буде потрібно відновити систему.

«Пропуск на вихід з в'язниці» - це документ, який ви можете пред'явити будь-якому, хто вважатиме, що ви здійснюєте незаконну діяльність, коли насправді ви проводите дозволене тестування. Нерідко траплялися ситуації, коли експерт (або група експертів) проводили тест на проникнення, а до них підходили нічого не знають про це охоронці, які вважали, що він опинився в неправильному місці в неправильний час.

У процесі виконання тестування на проникнення, команда проходить через п'ять етапів:

1. Дослідження. Збір інформації про цілі.
2. Перерахування (enumeration). Проведення сканування портів, використання технік і інструментів для ідентифікації виявлених систем і ресурсів.
3. Виявлення вразливостей (vulnerability mapping). Виявлення вразливостей в ідентифікованих системах і ресурсах.
4. Експлуатація. Спроби отримати несанкціонований доступ з допомогою в иявлених вразливостей.
5. Звіт керівництву. Надання керівництву документованих результатів тестування і пропозицій щодо усунення виявлених недоліків (контрзаходів).

Команді тестування на проникнення до початку тестування може бути наданий різний обсяг інформації про цілі, щодо якої здійснюється проникнення:

- нульова інформація. Команда НЕ має ніякої інформації про ціль і повинна починати з нуля;
- часткова інформація. Команда має деякі відомості про ціль;
- повна інформація. Команда має повну і детальну інформацію про ціль.

1.3.2 Типи тестування

Тестування вразливостей дозволяє виявити широке коло вразливостей в середовищі. Зазвичай воно виконується за допомогою інструментів сканування. На відміну від цього, при тестуванні на проникнення фахівці з безпеки експлуатують одну або декілька вразливостей, щоб продемонструвати замовникові (або керівництву компанії), що хакер реально може отримати доступ до корпоративних ресурсів.

Тестування безпеки середовища може виконуватися в різних формах, залежно від обсягу знань, які тестувальника дозволяється мати про середовище перед початком тестування, а також від ступеня дозволеної інформованості персоналу компанії про проведене тестування перед його початком.

Тестування може проводитися ззовні (з віддаленого місця) або зсередини (тобто тестувальник знаходиться в мережі компанії). Слід проводити обидва варіанти тестування, щоб зрозуміти як зовнішні, так і внутрішні загрози.

Тести можуть проводитися на основі сліпого методу, подвійного сліпого методу, або бути цілеспрямованими. При тестуванні *сліпим методом* (blind test), експерти знають тільки загальнодоступні дані перед початком тестування. Персонал компанії, що займається обслуговуванням мережі, і співробітники безпеки знають про проведеному тестуванні.

Подвійний сліпий метод тестування (double-blind test) (прихована оцінка) схожий на сліпий метод тестування, проте персонал компанії не ставиться до відома про проведеному тестуванні (включаючи співробітників безпеки). Це дозволяє перевірити не тільки рівень безпеки мережі, але й реакцію співробітників, реальне виконання ними функцій моніторингу журналів реєстрації подій, знання процедур реагування на інциденти та ескалації. Такий метод тестування є найбільш реалістичною демонстрацією ймовірності успіху чи провалу вірогідною атаки.

Для *цілеспрямованого тестування* (targeted test) можуть залучатися зовнішні консультанти і внутрішній персонал. При цьому здійснюється тестування, орієнтоване на конкретні області, що представляють інтерес для компанії. Наприклад, перед впровадженням нового додатка компанія може вирішити перевірити наявність у ньому вразливостей до того, як воно буде встановлено в промислову середовище. Іншим прикладом є тестування, орієнтоване на конкретні системи, що беруть участь, наприклад, у виконанні операцій дистанційного банківського обслуговування. Решта системи при цьому в тестуванні не беруть участь.

Важливо, щоб команда починала працювати, маючи тільки права звичайного користувача, що дозволить більш реалістично імітувати атаки. Команда повинна використовувати різні інструменти і методи атак, розглядати всі можливі уразливості - так, як це робитимуть справжні зловмисники.

Розглянемо деякі дії, що звичайно виконуються в процесі тестування на проникнення.

У споживачів послуг і продуктів інформаційної безпеки нерідко виникають питання: «Навіщо потрібен комплексний аудит інформаційної безпеки і, тим більше, тест на проникнення? Чому б просто не придбати який-небудь могутній засіб, або кілька потужних засобів і, посадивши за управління цими коштами сертифікованих фахівців, раз назавжди не вирішити проблему інформаційної безпеки нашої компанії?».

Досвідчені фахівці відповідають на ці питання приблизно так: «Одних лише технічних засобів захисту інформації недостатньо: компанія може витрачати на закупівлю, впровадження та обслуговування таких засобів мільйони рублів, доручати управління ними сертифікованим фахівцям, проте бюджет здійснення несанкціонованого проникнення до її найбільш цінним інформаційним активам буде продовжувати залишатися в межах декількох десятків тисяч».

Ефективність інформаційної безпеки залежить, насамперед, від ступеня усвідомлення ризиків і загроз, яким піддаються або можуть піддаватися інформаційні активи компанії. На вітчизняному ринку продуктів і послуг інформаційної безпеки кілька десятків консалтингових компаній і системних інтеграторів пропонують послугу під назвою «тестування на проникнення». У переважній більшості випадків, «тестування на проникнення» позиціонується як засіб пошуку та аналізу вразливостей (security assessment), при якому безпосереднє отримання доступу якимось цінним інформаційним ресурсом є побічною, другорядною завданням. При такому підході, як правило, проникнення як таке не відбувається. Компанії позиціонують тест на проникнення як здійснення проникнення до найбільш цінних і чутливим інформаційних ресурсів компанії Замовника (penetration testing). При такому підході, пошук і аналіз вразливостей є другорядним завданням.

1. Модель порушника: кваліфікований мотивований порушник:

– об'єднання традиційних моделей порушника «зовнішній порушник» і «внутрішній порушник» під загальною концептом «кваліфікованого мотивованого порушника»;
– простір впливу на об'єкти інформаційної захисту: лобовий, інтерактивний і фізичний вектори впливу;
– засоби захисту інформації очима кваліфікованого порушника, в розрізі pre-exploit - exploit - post-exploit. Класифікація вразливостей в контексті їх фактичної експлуатації;
– практичні приклади.

2. Арсенал засобів впливу кваліфікованого порушника на інформаційні об'єкти:

– root kit – система прихованого віддаленого управління – наріжний камінь кваліфікованого порушника, за допомогою якого порушник із «зовнішнього» перетворюється у «внутрішнього»;

– концепт «man in the middle», що надає змогу зломщикові отримувати контроль над усіма вузлами локальної обчислювальної мережі в межах типологічної однорідності;
– концепт «man in the box», що дозволяє зломщику здійснювати абсолютний контроль над захопленою інформаційною системою;
– практичні приклади.

3. Організаційні питання проведення робіт з тестування на проникнення:
– тестування на проникнення як вектор, який ініціює інформаційну безпеку в компанії замовника;
– цільові групи споживачів послуги тестування на проникнення.

з соціальною інженерією і спрямованих на користувачів корпорації.

1.4 Висновок

Аудит інформаційної безпеки - один з найбільш ефективних сьогодні інструментів для отримання незалежної та об'єктивної оцінки поточного рівня захищеності підприємства від загроз інформаційної безпеки. Крім того, результати аудиту дають основу для формування стратегії розвитку системи забезпечення інформаційної безпеки організації. Однак необхідно розуміти, що аудит безпеки - не разова процедура, вона повинна проводитися на регулярній основі. Тільки в цьому випадку аудит буде приносити реальну віддачу та сприяти підвищенню рівня інформаційної безпеки компанії.

Тестування на проникнення – оптимальний варіант наочної демонстрації ризиків і загроз інформаційній безпеці, звичайно ж, без нанесення будь-якої шкоди діяльності компанії.

Таким чином є необхідність розробки алгоритму та проведення тесту на проникнення для покращення інформаційної безпеки підприємства.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Тест на проникнення

Тест на проникнення (penetration test або скорочено pentest) - це практичний спосіб показати, наскільки захищена компанія від зазіхань на її конфіденційні дані та інших загроз для інформації. За кордоном також часто зустрічається термін етичний хакінг (ethical hacking).

Даний метод симулює набір «хакерських» атак, цілі яких - проникнення у внутрішню інфраструктуру мережі компанії, крадіжка та/або модифікація конфіденційних даних, порушення роботи критичних бізнес процесів компанії.

Такий захід є необхідним для будь-яких компаній, що залежать від інформації та обслуговуючих її систем інформаційних технологій (IT). Наприклад, робота банківської установи практично повністю залежить від функціонування процесних систем, а інтернет-магазин перестане здійснювати продажу у разі блокування його веб-сайту.

Приклади інцидентів застосовуються практично до будь-якої компанії і здатні спричинити за собою критичні наслідки для бізнесу аж до його закриття:

- попадання бази клієнтів в руки конкурентів;
- розголошення конфіденційних розробок компанії;
- крадіжка зловмисником бази даних бухгалтерії з контрагентами та фінансовими транзакціями компанії;
- крадіжка даних автентифікації для роботи з платіжними системами або системами «клієнт-банк» компанії;
- знищення резервних копій важливих даних компанії за тривалий період;
- втрата доступності критичних інформаційних систем в результаті dos або інших видів переривання в обслуговуванні.

З кожним днем все більше відчувається залежність від IT-технологій та інформації в будь-яких компаніях незалежно від напрямку їх діяльності.

Інциденти інформаційної безпеки, пов'язані зі зломами, часто стають критичними або навіть фатальними для безлічі компаній щорічно, а сьогодні стали актуальними і для України. Подібні інциденти, як правило, замовчуються, що створює певну атмосферу безпечності для інших компаній. Однак, деякі випадки все ж потрапляють у ЗМІ та публікуються на популярних новинних сайтах. Досить згадати гучний інцидент з несанкціонованим доступом до системи «клієнт-банк» одного з банків і великого оператора зв'язку в березні 2011 р, коли було завдано збитків у розмірі близько 7 млн. грн. Звичайно, завдяки оперативності профільних підрозділів МВС України та банківських працівників зловмисники були знайдені, але репутації банку було завдано істотної шкоди.

Сьогодні тестування на проникнення мало поширена послуга на українському ринку інформаційної безпеки, однак, практика проведення подібних тестів - звичайна справа для зарубіжних компаній або компаній орієнтованих на міжнародні стандарти. Дуже небагато українських компаній проводять такі заходи зважаючи на багато причин, серед яких є певні помилки. Розглянемо ці помилки більш детально.

Було встановлено, що тест на проникнення - це свого роду експрес-метод визначення слабких ланок у системі безпеки компанії. Для перевірки інформаційних систем і інфраструктури - проводять IT-тест на проникнення, обізнаності персоналу - соціальна інженерія, фізичної безпеки - тест проникнення на територію підприємства. Відповідно, результати тесту дають можливість визначити ефективність і достатність існуючих контролів безпеки в компанії.

Для такої перевірки залучаються зовнішні фахівці, по-перше, як і при будь-якому аудиті, необхідно отримати незалежну оцінку, що далеко не завжди можливо зусиллями тільки внутрішніх фахівців компанії. По-друге, мати на підприємстві висококваліфікованих і часто вузькоспрямованих фахівців не завжди доцільно.

При залученні зовнішніх фахівців дуже важливим залишається питання початкової підготовки та контролю проєкту на кожній стадії - для того щоб тестування не привело до реальних інцидентів. Таким чином, наприклад, необхідно забезпечити резервні копії для тестованих систем, детально обговорити сценарії і оцінити потенційні наслідки в разі успішної «атаки», проводити тестування у неробочий час для зменшення ризику зупинки бізнес процесу.

Не варто також забувати про основну мету, а саме вдосконалення системи безпеки компанії, яке починається вже після того, як проєкт закінчується. Таким чином, дуже важливим є аналіз результатів та відповідні реагування - усунення вразливостей в процесах, а можливо і зміна самих процесів, розробка нових контролів. Оцінка критичності тієї чи іншої загрози для компанії допоможе розставити пріоритети і усунути слабкі ланки, звівши при цьому до мінімуму ймовірність виникнення інцидентів безпеки.

Найчастіша помилка про тестування на проникнення це є його ціна. Більшість компаній готові витрачати мільйони на придбання різних IT-рішень і обслуговування цих потужних машин, які не працюють навіть на 30% своїх можливостей, але не готові витрачати адекватні гроші за впевненість у цілості свого бізнесу. У інформаційної безпеки є золоте правило, яке свідчить, що вартість захисту інформації ніколи не повинна перевищувати її вартість.

Середня стартова ціна на pentest в Україні коливається від 10 000 $ і зростає залежно від обсягів і опцій тесту, про що піде мова трохи нижче. Середня ціна за повноцінний комплексний проєкт може скласти близько 20 000 $ і навіть більше.

Витрати, пов'язані з тестом на проникнення, включають оплату праці експертів, підтримку спеціалізованого програмного забезпечення (ПЗ), устаткування та IT-послуг (наприклад, купівлю анонімних VPN каналів, створення фішингових сайтів і т.п.) і накладні витрати. У випадку з іноземними аудиторами витрати зростуть у зв'язку з більш високими цінами

на послуги та оплату праці, а також необхідністю додатково сплатити переїзд та проживання в готелі для виконавців.

Говорити про менші суми можливо тільки в разі зменшення обсягу та якості робіт, використанні некваліфікованих фахівців - любителів, сумнівного або зламаного ПЗ. У цьому випадку замовник просто даремно витрачає свій час і гроші і отримує замість послуги «галочку для керівництва».

Ще одна розповсюджена помилка це невміння фахівців ІБ відрізнити сканування вразливостей від тесту на проникнення. Насправді ці поняття являють собою різні послуги.

Сканування вразливостей проводиться спеціальними програмами-сканерами, які дозволяють в автоматичному режимі перевіряти мережевий периметр і веб-сайти компанії на наявність проломів. Безсумнівно, такий захід є одним з ключових етапів тесту на проникнення, що дозволяє знайти значну кількість потенційних вразливостей в системі, визначити відсутність патчів або інших проблем у захисті ІТ-систем.

Слід врахувати той факт, що логіка роботи даних сканерів не дозволяє виявити все, що може виявити команда професійних експертів. Значна кількість вразливостей залишається за рамками охоплення кожного з відомих сканерів.

Тест на проникнення передбачає системний підхід, пошук та аналіз інформації з різних джерел, проведення атак методами соціальної інженерії, глибоке сканування мережі та сайтів компанії різними методами та інструментами, перевірку реакції співробітників на виникнення інцидентів ІБ, що дозволяє більш адекватно оцінити стан інформаційної безпеки, а також необхідних процесів ІБ.

Інша помилка: Тест на проникнення це довго і незрозуміло. Що робити із результатами.

На жаль, відсутність ризику менеджменту в більшості українських компаній є фактом сьогоднішнього дня. В дійсності, результати тесту дозволяють отримати вхідні дані для аналізу ризиків ІТ, оптимізувати витрати

на інформаційну безпеку (надсилати бюджет саме на проблемні області), коригувати стратегію IT з бізнес-стратегією компанії з урахуванням виявлених ризиків. Стосовно тривалості, залежно від обсягів тесту (кількості цільових об'єктів Замовника) тривалість варіюється в межах від 3 до 8 тижнів.

2.1.1 Методи етичного хакінгу

Організований процес етичного хакінгу, на відміну від реальних зловмисників, відрізняється тим, що команда тестерів дотримується певних етичних правил при проведенні всіх робіт: будь-які небезпечні дії здійснюються тільки за попереднім погодженням із замовником, весь процес сканування прозорий і спланований, робота критичних бізнес-процесів не порушується, а в кінці тесту замовник отримує об'єктивний звіт про стан справ в його системі безпеки в термінах, зрозумілих не тільки IT фахівцям, але і бізнесу.

Існування різних методик проведення тестів на проникнення не скасовує творчої складової процесу, що вимагає від команди, яка виконує його, глибоких пізнань у сфері IT-безпеки і в той же час - вміння мислити нестандартно, застосовувати методи соціальної інженерії, збирати та аналізувати інформацію.

Найбільш використовувані методології Етичного хакінгу :

- Information Systems Security Assessment Framework (OISSG);
- The Open Source Security Methodology Manual (OSSTMM);
- NIST SP800-115 Technical Guide to Information Security Testing and Assessment;
- ISACA Switzerland - Testing IT Systems Security With Tiger Teams;
- The Information Systems Security Assessment Framework (ISSAF);
- OWASP Testing Methodology;
- BSI - Study A Penetration Testing Model;
- Penetration Test Framework (PTF).

Існують як відкриті, так і комерційні методології проведення тестів на проникнення, здатні при дотриманні всього процесу забезпечити гарантовану якість послуги. Однак, на практиці використання лише однієї методології не є доцільним, як правило, вони використовуються модульно з необхідним доопрацюванням. Деякі методології вже застаріли і не враховують стрімкі темпи розвитку IT, а деякі охоплюють тільки організаційні моменти, не вдаючись у технічні деталі, інші ж націлені лише на певні технології і практично жодна методологія не спроможна врахувати особливості української сфери IT-технологій.

Як правило, всі методології, з невеликими відхиленнями передбачають наступний сценарій проведення тесту на проникнення:

1 Ініціалізація;
2 Підписання угоди про конфіденційність;
3 Одержання листа про початок тестування від замовника;
4 Визначення умов та обмежень тестування;
5 Формування робочої групи;
6 Підписання статуту проєкту;
7 Планування тесту на проникнення;
8 Збір публічно доступних даних;
9 Збір інформації про цільові системи;
10 Аналіз відкритої інформації про організацію;
11 Вивчення базової інформації про мережевий інфраструктурі;
12 Аналіз соціальних мереж;
13 Аналіз вакансій, резюме на hr-сайтах;
14 Аналіз технічних форумів;
15 Сканування;
16 Сканування портів;
17 Визначення додатків і веб додатків;
18 Визначення операційних систем;
19 Ідентифікація мережевих маршрутизаторів і міжмережевих екранів;

20 Пошук вразливостей (автоматизовані сканування і ручний аналіз);

21 Аналіз вразливостей;

22 Проникнення в системи;

23 Написання та надання звіту;

24 Очищення систем від наслідків тесту.

2.1.2 Планування тесту на проникнення

Тест на проникнення є комплексним проєктом і може включати в себе кілька видів робіт з яких і формується ціна і терміни. На даному етапі також обумовлюються обмеження та ролі учасників.

1. Слід визначити підхід до проведення тесту: білий (White box), чорний (Black Box) або сірий (Grey Box) ящик.

Повний доступ до інформації (White box)

Виконавець має доступ до систем і своєму розпорядженні повну інформацію про них, фактично така модель тестування використовується як частина організаційно-технічного аудиту організації IT та передбачає аналіз процесів і процедур.

Не має доступу до інформації (Black Box)

Імітує групу хакерів, які мають тільки назву компанії і практично нульові відомості про цільові системи.

Частковий доступ до інформації (Grey Box)

Передбачає імітацію хакерів, які володіють інформацією частково (наприклад про діапазон IP адрес, Web сайтах, фізичне місце розташування, ідентифікаторах бездротових мереж тощо), а також можливо, доступом з низьким рівнем привілеїв в деякі тестовані системи.

Дані моделі визначають початкові знання про тестовану систему у виконавця тесту. Варто згадати, що більшість методологій розглядають підхід Black Box, як тестування кваліфікації самого виконавця тесту. З нашої точки зору даний підхід просто подовжує першу фазу тесту - збір відомостей про

цільові системи. Так що по суті замовник побічно платить за оцінку кваліфікації самого аудитора.

2. Також визначається тип і кількість тестованих систем. Найбільш часто визначаються наступні параметри для зовнішнього тестування:

- *тестування периметра мережі*. Визначається кількістю IP адрес;
- *тестування WEB сайтів*. Визначається кількістю URL сайтів;
- *тестування спеціалізованих додатків*. Наприклад, додаток «Клієнт-банк» або будь-яке інше клієнтське ПЗ, яке взаємодіє з серверами компанії;
- *тестування співробітників на стійкість до методів соціальної інженерії* сюди входять спроби фішинг (обдзвін ключових співробітників з метою отримання паролів), проведення фішингових атак, використання вірусів для отримання доступу до систем, пошук інформації в смітті компанії, і інші методи;
- *фізичне проникнення на територію компанії*. Може включати злом замків або проникнення обманом під виглядом обслуговуючого персоналу з метою отримання інформації, карток і кодів доступу, ключів, ноутбуків, телефонів, паролів, закладки жучків, проникнення в серверну і т.д.;
- *тестування бездротових мереж*. Визначається кількість точок доступу. Також можлива опція установки підставної точки доступу з метою перехоплення трафіку користувачів.

На даному етапі можна завершити весь проєкт або продовжити pentest шляхом аналізу внутрішньої мережі (тут можливі тільки підходи білого або частково сірого ящика). У такому випадку імітується атака з боку інсайдера.

Опції тестування можуть включати:

- тестування внутрішнього периметра мережі. Повний тест на проникнення або ж проведення автоматизованого сканування вразливостей внутрішніх ресурсів компанії. Визначається кількість IP адрес, веб-сайтів і додатків;

- аналіз змін мережевих пристроїв, додатків і серверів на відповідність стандартам безпеки. Виробники, що випускають обладнання та програми, визначають власні рекомендації з безпеки. Аналіз проводиться з метою виявлення відхилень у рекомендаціях;
- аналіз коду веб-сайтів. Код перевіряється на наявність вразливостей типу SQL injection, command injection, file inclusion, DoS, наявність несанкціонованих закладок, недоліків в архітектурі та ін.
- аналіз коду додатків. Код перевіряється на наявність вразливостей типу Buffer overflow, DoS, на наявність несанкціонованих закладок, недоліків в архітектурі та ін.;
- аудит мобільних пристроїв. Аналіз безпеки використання телефонів, смартфонів, планшетів, також пристроїв зберігання даних, таких як USB та інших мобільних пристроїв.

3. Також важливо визначити порядок надання звітності. Кваліфікований аудитор зможе надати розгорнуту інформацію про виконану роботу для менеджменту в зрозумілій формі. З найбільш доцільних варіантів:

- один результуючий звіт після закінчення тестування;
- надання окремого звіту відразу при виявленні критичної уразливості;
- проміжні звіти раз на 2-3 дні.

4. Необхідно також визначити наступні організаційні моменти:

- канали зв'язку для обміну інформацією між замовником і тестерами, цілком зрозуміло, що вони повинні бути зашифровані;
- відповідальних осіб з боку виконавця і замовника;
- порядок дій у разі виникнення інцидентів, пов'язаних з проведенням тестування;
- обмеження тестування (наприклад, тільки у вихідні дні, тільки безпечні перевірки для певних систем і т.д).

Усі заходи з тестування проводяться тільки після підписання договору, а також угоди про нерозголошення з виконавцями. Виконавець зі свого боку проводить внутрішню підготовку до тесту: інструктаж персоналу, організацію

спільної роботи, підготовку необхідного обладнання та ПЗ, каналів зв'язку та інше.

2.1.3 Збір інформації

Першочерговим завданням аудиторів на даному етапі є збір якомога більшої кількості інформації про тестовану систему і про співробітників компанії. Найчастіше вже на даному етапі можливе виявлення критичних вразливостей, таких, як забуті або мало використовувані сервіси, які не потребують авторизації і дають доступ у внутрішню мережу, опубліковані конфіденційні дані, паролі та інша критична інформація.

Пошук інформації відбувається в доступних джерелах вручну, а також за допомогою спеціалізованих інструментів. В обсяг робіт, як правило, входить пошук інформації в таких джерелах:

- пошукові системи;
- соціальні мережі і сайти знайомств;
- каталоги підприємств;
- новинні сайти;
- корпоративні сайти компанії замовника, сайти клієнтів і партнерів;
- сайти пошуку роботи;
- бази даних whois;
- dns сервера компанії;
- аналіз маршрутів і виявлення мережевого обладнання;
- чорні списки спамерів;
- аналіз e-mail листів;
- дзвінки в call-центр компанії з метою отримання інформації про ключових співробітниках компанії, про структурі компанії і технологіях;
- аналіз метаінформації в документах, розміщених на сайтах компанії;
- безпосереднє сканування мережі різними інструментами для виявлення ip-адрес, портів, версій працюють сервісів і операційних систем;

– перегляд сміття компанії з метою знайти конфіденційну інформацію і інші методи.

Як вже було сказано вище, підхід «тільки сканування вразливостей» не враховує всієї інформації, зібраної на етапі розвідки. Озброївшись же повним набором інформації можна приступати до сканування вразливостей, що в подальшому дасть більш повну картину про можливі недоліки в захисті.

2.1.4 Сканування системи та пошук вразливостей

Засоби аналізу захищеності (також відомі як сканери безпеки) являють собою інструменти управління захистом, які:

– проводять всебічні перевірки систем, намагаючись локалізувати уразливості захисту;
– генерують звіт про число, природі і силі цих вразливостей;
– дозволяють системному адміністраторові визначати ефективність адміністрування системи захисту організації;
– дозволяють системному адміністраторові визначати стан захисту системи в конкретний час;
– у деяких випадках, як тільки відбувається інцидент, дозволяють дослідникам визначити точку входу і маршрут хакера або порушника.

Системи аналізу захищеності доповнюють системи виявлення атак:

– вони дозволяють системним адміністраторам більш активно захищати свої системи шляхом знаходження і виявлення дірок захисту до того, як хакери зможуть використовувати їх. Системи виявлення атак є за природою реактивними;
– вони здійснюють контроль за хакерами, націлює на системи, в надії перервати атаки до того, як система буде пошкоджена.

Підхід до аналізу захищеності.

Аналіз захищеності на рівні додатку

Аналіз захищеності на прикладному рівні використовує пасивні, що не роблять помітного впливу методи для перевірки конфігурації в межах

прикладних програмних засобів на предмет наявності помилок, які, як відомо, мають місце бути.

Аналіз на системному рівні

Аналіз на системному рівні використовує пасивні, що не роблять помітного впливу на роботу, методи для перевірки налаштувань і конфігурації системи на наявність помилок, які можуть викликати проблеми з захистом. Ці перевірки звичайно оточують нутрощі системи і включають такі речі, як права доступу до файлів і права спадкування, а також використані чи ні patches для усунення вразливостей операційної системи.

Більшість систем аналізу захищеності проводять аналіз паролів, як частину своєї роботи. Аналіз паролів складається з запуску зломщиків паролів проти файлів з паролями, що використовують добре відому атаку для того, щоб швидко визначити місцезнаходження уразливості, неіснуючі або, з іншого боку, слабкі паролі.

Переваги:

– він дає дуже точну, конкретну для даного хосту картину дірок захисту.
– він охоплює діри захисту, які не перебувають протягом аналізу на системному рівні.

Недоліки:

– ці методи аналізу залежать від типу конкретної платформи і, таким чином, вимагають точної конфігурації кожного типу хосту, використовуваного організацією.
– експлуатація та оновлення часто вимагають набагато більше зусиль, ніж при аналізі на мережевому рівні.

Аналіз на рівні заданої мети

Цільовий аналіз (також відомий як контроль цілісності файлів) використовує пасивні, що не роблять помітного впливу на роботу методи для перевірки цілісності системи і файлів даних, а також об'єктів системи та їх атрибутів (наприклад, потоки даних, бази даних і ключі реєстру). Системи цільового аналізу використовують криптографічні перевірки контрольних сум

для того, щоб отримати докази підробки для найбільш важливих системних об'єктів і файлів. Message-digest алгоритми засновані на хеш-функціях, які володіють тим властивістю, що навіть незначні зміни у вхідних даних функції створюють великі відмінності в результаті. Це означає, що зміна в потоці даних призведе до того, що message digest алгоритм створює значну зміну в контрольній сумі, що генерується алгоритмом. Ці алгоритми є криптографічно сильними; тобто, при заданому конкретному вхідному значенні (величиною), практично неможливо зрівнятися з іншим вхідним значенням для алгоритму, яке буде створювати ідентичне вихідне значення. Це запобігає найбільш поширену атаку проти порівняно простих CRC (циклічного надлишкового коду) контрольних сум, при яких хакери маскують зміни в файлах шляхом зміни змісту файлу, так що однакова контрольна сума генерується як для оригінального, так і для підробленого файлу.

Системи цільового аналізу працюють по замкнутому циклу, обробляючи файли, системні об'єкти і атрибути системних об'єктів з метою отримання контрольних сум; потім вони порівнюють їх з попередніми контрольними сумами, відшукуючи зміни. Коли зміна виявлено, продукт посилає повідомлення системі виявлення атак, яка записує проблему, фіксуючи час, відповідне ймовірного часу зміни.

Аналіз на мережевому рівні

Аналіз вразливостей на мережевому рівні використовує активні, що не роблять помітного впливу на роботу мережі методи для визначення того, є чи ні дана система вразливою до набору атак. При аналізі на мережевому рівні, широкий діапазон сценаріїв атак використовується проти обраної системи (систем), потім результати аналізуються для того, щоб визначити вразливість системи до атаки. У деяких випадках аналіз на системному рівні використовується для сканування проблем, характерних для мережі (наприклад, сканування портів). Аналіз вразливостей на мережевому рівні часто використовується для випробувань на проникнення (особливо, при тестуванні MCE) та аудиту захисту.

Переваги:

- він знаходить "дірки" захисту на цілому ряді платформ і систем;
- оскільки аналіз вразливостей на мережевому рівні не залежить від платформи і типу системи, його можна легко і швидко задіяти;
- оскільки він не передбачає доступу на системному рівні, його легко використовувати з організаційної точки зору;

Недоліки:

- оскільки він не враховує уразливості, характерні для платформи, він часто менш точний, ніж аналіз на системному рівні;
- він може впливати на продуктивність мережі і її характеристики.

Інтегрований аналіз

Інтегрований аналіз вразливостей об'єднує активний аналіз на мережевому рівні з пасивними методами аналізу на системному рівні, часто інтегруючи їх за допомогою функції централізованого управління. Тут варто зазначити, що мережеві середовища, що працюють під ОС Windows NT, що не розпізнають чітку межу між доступом на рівні ОС і доступом на мережевому рівні.

Переваги:

- він комбінує гідності аналізу на системному рівні - більш досконалу ідентифікацію вразливостей, характерних для платформ, з можливостями аналізу на мережевому рівні з ідентифікації проблем через широкий діапазон уражених систем і мереж;

Недоліки:

- експлуатація та супровід модулів комбінованого аналізу вимагає досить значних зусиль;

Місцезнаходження засобів аналізу

Збір даних - це перший крок у процесі аналізу вразливостей; аналіз даних - другий крок. При інсталяції великий, складної мережі корисно організувати аналіз вразливостей, використовуючи архітектуру агент-менеджер. Ця архітектура є особливо корисною там, де мережі є

гетерогенними (різнорідними), тобто з широким діапазоном платформ з різними ОС.

Переваги:

– централізовані архітектури можуть встановлювати агентів для платформ з конкретною ос, а також змінювати область охоплення і глибину аналізу, спираючись на загрозу мережевого оточення;

Недоліки:

– розподілені архітектури вимагають додаткових віддалених (дистанційних) привілеїв на мережі, які скануються;

Для відстеження публікованих повідомлень про вразливості програмного забезпечення можна використовувати такі ресурси:

– securityfocus http://www.securityfocus.com/archive/1
– багтрак seclists.org http://seclists.org/bugtraq/
– база даних вразливостей cve http://www.cvedetails.com/
– open source vulnerabilities data base (osvdb) http://osvdb.org/
– база даних вразливостей secunia http://secunia.com/community/advisories/historic/
– база даних вразливостей bugs collector (в тому числі невиправлених) https://bugscollector.com/
– база даних xss-вразливостей xssposed.org (у тому числі невиправлених) https://www.xssposed.org/
– бюлетені безпеки microsoft https://technet.microsoft.com/security/bulletin/

Виконати установку (перевірку) безпечних налаштувань для операційних систем і програмного забезпечення допоможуть інструкції National Checklist Program і CIS Security Benchmarks.

Генерація звітів

Генерація звітів при аналізі вразливостей є ключем для розуміння і усунення дірок захисту. Генерація звітів представляє можливість для документування стану захисту сканованої системи, для публікації проблем для відповідного рівня управління для того, щоб призначити ресурси та

відповідальні сторони для їх усунення, і для доведення до всього персоналу організації всієї важливості захисту системи і способів її забезпечення. Надані опції включають змінні формати генерації звітів (у разі HTML пропонується можливість для вибіркової "прокрутки" до більш точного рівня бажаної деталізації) і рівні деталізації, забезпечуючи значні кількості додаткової інформації про уразливість і відповідних fixes.

Планування злому:

- аналіз отриманої інформації;
- розробка сценаріїв злому інформаційної системи;
- розробка і модифікація експлойтів ;
- підготовка необхідного інструментарію пентеста ;
- експлуатація вразливостей;
- верифікація і дослідження вразливостей;
- проведення атак на компоненти іт-інфраструктури;
- підбір паролів;
- визначення взаємодії додатків;
- підтвердження виявлених вразливостей;
- збір доказів;
- підготовка звітних документів
- розробка та узгодження рекомендацій;
- оформлення та презентація звіту;
- результати оцінки захищеності

Результатом проєкту з тестування на проникнення є інформація про поточний рівень захисту, що існують в інфраструктурі уразливість і детальні рекомендації щодо їх усунення.

По завершенні проєкту Замовник отримує Звіт про оцінку захищеності периметра інформаційних систем.

Хакінг і тестування на проникнення

Розвідка та збір інформації перед тестуванням на проникнення (pentest).

Тестування на проникнення - метод оцінки безпеки комп'ютерних систем або мереж засобами моделювання атаки зловмисника.

Способи проведення pentest:

- Автоматизоване тестування (сканери) ;
- Ручне тестування ;
- Комбінований метод.

Залежно від обраних систем на даному етапі проводиться сканування вразливостей різними програмами-сканерами. Спеціалізація подібних сканерів може бути орієнтована на тестування периметра мережі, web-сайтів, окремих додатків і сервісів, таких як бази даних, VPN-пристрої, пристрої IP-телефонії та інших.

Важливо відзначити, що будь-який інструмент видає певну кількість помилкових спрацьовувань, таких як виявлення помилкової уразливості або навпаки пропуск уразливості, коли вона дійсно існує. Щоб збільшити ймовірність знаходження необхідно проводити сканування двома-трьома сканерами. Також для знаходження вразливостей проводиться аналіз версій використовуваного ПЗ: часто вже не оновлене або застаріле ПЗ має опубліковані уразливості, що не знайдені жодним з сканерів.

2.1.5 Проникнення до системи

Знайдені потенційні уразливості повинні бути перевірені вручну, щоб відфільтрувати всі помилкові спрацьовування.

Для злому вразливих IT-систем використовується різний спеціалізований інструментарій, експлойти в публічному доступі на хакерських сайтах. У деяких випадках потрібна власна розробка вірусів і експлойтів для проникнення всередину мережі.

Також відзначимо, що в хакерському підпіллі існує ринок продажу 0-day експлойтов і вразливостей. Це ті уразливості, які ще не були виявлені і опубліковані виробником ПЗ. Теоретично можливі варіанти покупки подібних експлойтов, але юридично подібну покупку здійснити складно, так як дані

продукти продаються за готівку або за безготівкові перекази через популярні платіжні системи без будь-якої документації, гарантій, ліцензій.

Всі вектори проникнення, включаючи соціальну інженерію, фізичне проникнення, бездротові мережі та інші атакуються на цьому етапі і розвиваються надалі до максимально можливого рівня доступу.

Результати кваліфіковано проведеного тесту на проникнення продуктивні для декількох ланок компанії, що його замовила. Вищий менеджмент отримує інтегровану оцінку захищеності інформаційної системи і може прийняти рішення про ефективність витрат на IT-безпеку і сформувати підходи до подальшого фінансування даного напрямку. Керівництво IT отримує в руки два набори даних для планування своєї діяльності. Перший - документовані звіти про найбільш істотні вразливості периметра. Впевнений, якщо тест буде кваліфікованим, то і звіти будуть такими.

Обов'язково пропозиції розміщенні в підсумковому звіті щодо підвищення захищеності периметра стануть істотним доповненням для коригування планової діяльності підрозділу IT-безпеки. Надзвичайно корисними будуть як результати оцінки дій персоналу при виникненні подій безпеки, так і самі спостереження за співробітниками і отримані в ході нього оцінки їх професійної підготовки.

Перший тест, його висока продуктивність багато полягатиме в комплексності використаних пен-тестерами технологій, охопленням ними всіх можливих векторів атак. Якщо ставиться завдання на глибоке проникнення в корпоративні системи, порушення цілісності та конфіденційності даних в них, то в рамках фіксованого бюджету краще зосередитися на найбільш повному і різнобічному дослідженні периметра. І ні в якому разі не виключайте з тесту соціальну інженерію. Її дані можуть виявитися дивні.

2.1.6 Підготовка звіту та очищення систему від наслідків тесту

Після проведення всіх необхідних робіт по проникненню повинен бути наданий звіт, який надалі презентується керівництву компанії і фахівцям IT та

ІБ. Деякі стандарти пред'являють цілком певні вимоги до звіту, чим можна керуватися при його складанні. Практика ведення бізнесу в Україні показує, що найбільш оптимальною структурою звіту є його розбиття на 3 рівні: для вищого керівництва, для менеджерів ІБ і для технічних фахівців.

Звіт повинен містити повне перерахування проведених робіт та їх результат, знайдені вразливості з докладним описом сценаріїв атак, докази злому систем та рекомендації щодо усунення вразливостей в технічних системах та ІТ-процесах компанії.

Після проведення тесту можливі залишкові сліди тесту, так звані артефакти, які необхідно усунути. Наприклад, якщо був отриманий доступ до якої-небудь системи, то необхідно провести зміну паролів для всіх її користувачів, у разі використання вірусів їх також слід видалити, і т.д.

Слід також зазначити, що тест на проникнення не дає 100% гарантії захищеності систем: існують 0-day уразливості, про існування яких відомо лише обмеженому колу осіб. Подібними уразливими користуються хакерські спільноти, на зразок прославлених Anonymous. На підпільних сайтах за певну суму можна придбати експлойти для цих вразливостей, і в разі достатніх ресурсів у зловмисника, питання злому стає справою часу.

Щоб зменшити ймовірність і наслідки злому необхідна організація підходу «defense in depth» (глибокоешелонованого захисту) і високої доступності, налагодження всіх необхідних процесів для реакції на спроби злому та зменшення наслідків атаки. Важливими елементами є організація наступних процесів:

- установка оновлень в системах і ПЗ;
- управління ризиками для критичних бізнес процесів і систем;
- управління змінами;
- моніторинг та реєстрація подій безпеки;
- реакція на інциденти в разі виявлення злому;
- розслідування інцидентів (forensics) з юридично правильним оформленням доказів;

– навчання співробітників правил ІБ;
– управління резервуванням і відновленням інформації.

Для організації всіх необхідних процесів необхідно обрати один з підходів до забезпечення інформаційної безпеки, пропонований міжнародними, а тепер для певних галузей і національних стандартів.

Існуючі методології проведення тесту на проникнення:

– Стандарт Information Systems Security Assessment Framework (ISSAF);
– Стандарт NIST 800-42 Guideline on Network Security Testing;
– Стандарт Open Source Security Testing Methodology Manual (OSSTMM);
– OWASP Testing Guide_V3;
– PTES Technical Guidelines;
– Fuzz testing (фаззінга). Фаззінг - методика тестування, при якій на вхід програми подаються невірні, непередбачені або випадкові дані.

DNS (англ. Domain Name System - система доменних імен) - комп'ютерна розподілена система для отримання інформації про доменах. Найчастіше використовується для отримання IP-адреси за назвою хосту (комп'ютера або пристрою), отримання інформації про маршрутизації пошти, які обслуговують вузлах для протоколів в домені (SRV-запис).

DNS створений для зручності людей. А все, що створено для зручності людей в комп'ютерному світі, є вразливим.

DNS володіє наступними характеристиками:

– розподіленість адміністрування;
– розподіленість зберігання інформації;
– кешування інформації;
– ієрархічна структура;
– резервування;

DNS-записи:

– запис a (ipv4 address record) ;
– запис aaaa (ipv6 address record);
– запис cname (canonical name record)

- запис mx (mail exchange)
- запис ns (name server)
- запис ptr (pointer)
- запис soa (start of authority)
- srv-запис (server selection)

Інструменти для роботи з DNS:

- nslookup
- dig
- host

Програми для легальної роботи також можуть бути використані і для зловмисної діяльності.

Nslookup (англ. name server lookup - пошук на сервері імен) - утиліта, що надає користувачеві інтерфейс командного рядка для звернення до DNS. Дозволяє задавати різні типи запитів і запитувати довільно вказуються сервера. Розроблено в складі пакету BIND (для UNIX-систем). Утиліта експортована на Windows безпосередньо фірмою Microsoft і поставляється разом з операційною системою.

2.2 Розробка сценарію на проникнення

2.2.1 Введення до роботи

Роботи проводяться згідно договору між BLA (далі - Замовник) та Агентства аудиту (далі – Виконавець), всього 35 робочих днів.

Основна мета робот - забезпечити менеджмент підприємства актуальними і найбільш повними даними про стан захищеності внутрішніх і зовнішніх інформаційних ресурсів, каналів передачі даних та інформаційно-телекомунікаційних мереж підприємств, що входять в групу.

Даний документ висловлює повну згоду і підтримку керівництва BLA в проведенні втручання в роботу інформаційних систем і бізнес процесів BLA в обсязі визначеному в наступному пункті «Область дії та обмеження».

2.2.2 Область дії та обмеження

Згідно з вимогами Замовника для проведення аудиту обрано такі обмеження:

1 Виконавець володіє базовими знаннями про тестовані системи - варіант «сірий ящик». Замовник може в робочому порядку надавати додаткову інформацію Виконавцю за своїм бажанням з метою проведення об'єктивного і всебічного аудиту;

2 Роботи проводяться тільки щодо наступних об'єктів аудиту(таблиці 2.1 і 2.2):

Таблиця 2.1 Зовнішні IP адреси

п / п	IP	Сервіс
1	10 .91.175.130	АСК
2	10 .91.175.132	SAP
3	10 .91.175.131	OpenVPN
4	10 .91.175.131	OpenVPN

Таблиця 2.2 Внутрішні IP адреси

п / п	Внутрішній IP	Сервіс
1	20.112. 8.163	ASCU
2	20.112. 97.44	ASCU
3	20.112. 8.165	ASC
4	20.112. 98.60	ERP-PRD
5	20.112. 98.2	SAP router
6	20.112. 48.144	ДГЕ
7	20.112. 48.145	
8	20.112. 48.146	
9	20.112. 48. 214	Мега білінг
10	20.112. 98.19	Фін
11	20.112. 97.41	

- Зовнішній WEB сайт: http: // bla. com. ua
- Внутрішні WEB сайти: http://www.bla2.ua/
- Адреси співробітників для проведення фішингової розсилки (всього 18 e-mail):
    1) 1bla.com;
    2) 2bla.com;
    3) 3bla.com;
    4) 4bla.com;
    5) 5bla.com;
    6) 6bla.com;
    7) 7bla.com;
    8) 8bla.com;
    9) 9bla.com;
    10) 10bla.com;
    11) 11bla.com;
    12) 12bla.com;
    13) 13bla.com;
    14) 14bla.com;
    15) 15bla.com;
    16) 16bla.com;
    17) 17bla.com;
    18) 18bla.com.

Контактні дані співробітників, для проведення соціальної інженерії – дзвінків, вибираються і узгоджуються в робочому порядку зі списку співробітників BLA на етапі проведення відповідних робіт. SSID бездротових точок доступу за адресою м. Дніпро, вул. Пушкіна, 13 для проведення аудиту:

- WiFi-USERS
- DCU
- AS
- MD

Аудит контрольованого периметра включає спроби проникнення в наступні приміщення за адресою: м. Дніпро, вул. Пушкіна, 13:

- Приймальна і кабінет генерального директора - для установки макета закладного пристрою;
- Приймальна і кабінет директора з фінансів - Для установки макета закладного пристрою;
- Одне з архівних приміщень договірного відділу (архіви - кабінети № 9, 10) - для зміни інформації в договорах
- Всі операції здатні порушити функціонування критичних бізнес процесів додатково авторизуються і проводяться в час, обумовлений з Замовником;
- Замовник не повідомляє свій персонал про проведення аудиту, з метою перевірки реакції співробітників відповідних підрозділів та дотримання ними внутрішніх процедур;
- Для точності надаються результати сканування портів і версій сервісів, а також кожен тип сканування вразливостей проводиться не менше ніж 2-ма інструментами;
- У разі успішної експлуатації уразливості атака проводиться до отримання максимально можливого доступу до наступних внутрішніх систем: SAP ERP, База даних ORACLE, АСК.
- Передбачені наступні види звітності:

1) за результатами аудиту представляється звіт з експертним висновком та рекомендаціями щодо зниження / усуненню ризиків реалізації загроз;

2) за бажанням Замовника можуть представляються усні проміжні звіти про стан проєкту і основних потенційних вразливості.

З метою забезпечення конфіденційності обміну інформацією між Виконавцем та Замовником встановлюються наступна процедура обміну конфіденційними даними:

- Обмін конфіденційними даними відбувається по електронній пошті на адреси контактних осіб Виконавця та Замовника. Конфіденційні дані

при цьому шифруються із застосуванням алгоритму AES-256, установкою пароля не менше 10 символів і упаковуються в RAR архів. Пароль дешифрування висилається через смс повідомлення на телефон зі списку контактних осіб. Пароль і зашифрований архів ніколи не передаються по одному каналу.

Дії у разі виникнення інцидентів:

– Виконавець негайно зв'язується з контактною особою Замовника, надає повну інформацію по причинам, які викликали інцидент, всі дії, що викликали інцидент негайно припиняються. Надалі Замовнику надається повний технічних звіт у письмовій формі про причини і дії, що викликали інцидент.

2.2.3 Алгоритм проведення тесту на проникнення

У таблиці 2.3 приведений план-графік проведення тесту на проникнення.

Таблиця 2.3 План-графік проведення penetration test

№	Назва робіт	Інструменти	Терміни
	1	2	3
1 Зовнішня пасивна розвідка - збір відомостей про Замовника з мережі Internet, базові запити про мережу та сайти			
1.1	Складання профілю компанії	Сайти замовника, довідники підприємств (Allbiz.info, Yellowpages.ua та ін.), Пошукові системи (Google), новинні портали (Korrespondent, Finance.ua)	22.08 - 23.08

Продовження таблиці 2.3

	1	2	3
1.2	Пошук інформації про інформаційну систему замовника в публічному доступі	Сайти замовника, сайти клієнтів і партнерів замовника, пошукові системи (Korrespondent, Finance.ua, новини Google), сайти пошуку роботи (rabota.ua, job.ukr.net, trud.ua, hh.ua, work.ua), аналіз заголовків електронних листів, сканування метаінформації на сайтах (FOCA)	22.08 - 27.08
1.3	Збір інформації про співробітників	Соціальні мережі (Linkedin, Facebook)	22.08 - 27.08
1.4	Дослідження реєстраційних даних про IP-адреси і автономних системах	BGP - bgp.he.net, WHOIS - www.ripe.net, параметри IP - ip.robtex.com, історія параметрів IP - domains.checkparams.com, перегляд чорних списків спамерів - mxtoolbox.com	22.08 - 23.08
1.5	Дослідження реєстраційних даних про DNS домени та імена	WHOIS, DNS записи - dns.robtex.com, історія параметрів DNS - domains.checkparams.com, перевірка фішингових доменів - UrlCrazy	22.08 - 23.08
1.6	Базове дослідження WEB серверів	Httprint, хостинг, сайти на одному IP, доступність сайту, перевірка на віруси, CMS	27.08

Продовження таблиці 2.3

	1	2	3
2 Зовнішня активна розвідка - сканування мережі замовника, активне дослідження мережі та сайтів			
2.1	Сканування відкритих портів TCP, UDP	NMAP, Angry IP scanner	22.08 - 30.08
2.2	Ідентифікація сервісів і версій ПЗ на відкритих портах, ідентифікація версій операційних систем	NMAP, AMAP	28.08 - 30.08
2.3	Відмалювання карти мережевого периметра (карти маршрутів і мережевих пристроїв)	Трасування ICMP, TCP (NMAP), Розвідувальне ПЗ (Maltego)	28.08 - 29.08
2.4	Прямий опитування DNS серверів	Основні типи записів - nslookup, dnsdataview, пошук піддоменів і хостів - dnsmap, Dnsdict6	28.08 - 30.08
2. 5	Виявлення директорій і скриптів на WEB сайтах	Dirbuster	29.08 - 30.08
2.6	Опитування поштових серверів для виявлення поштових скриньок	Підготовка словника, Mail list validator, ePochta Extractor	29.08 - 18.09
3 Зовнішнє виявлення вразливостей в периметрі - сканування вразливостей в мережі і в сайтах			
3.1	Сканування вразливостей мережевого периметра	Nexpose Express, Nessus	02.09 - 04.09

Продовження таблиці 2.3

	1	2	3
3.2	Сканування вразливостей сайтів	Acunetix, W3af, BurpSuite, Arachni	02.09 - 04.09
3.3	Аналіз застарілих версій ПЗ сервісів, які мають опубліковані уразливості	Сайти постачальників, www.cvedetails.com, exploit-db.com, 1337day.com	02.09 - 04.09
5 Внутрішня активна розвідка - сканування мережі замовника, активне дослідження мережі та сайтів			
5.1	Сканування відкритих портів TCP, UDP	NMAP	04.09 - 06.09
5.2	Ідентифікація сервісів і версій ПЗ на відкритих портах, ідентифікація версій операційних систем	NMAP, AMAP	04.09 - 06.09
6 Внутрішнє виявлення вразливостей в периметрі - сканування вразливостей в мережі і в сайтах			
6.1	Сканування вразливостей мережевого периметра	Nexpose Express, Nessus	09.09 - 12.09
6.2	Сканування вразливостей сайтів	Acunetix, W3af, BurpSuite, Arachni	09.09 - 13.09
6.3	Аналіз застарілих версій ПЗ сервісів, які мають опубліковані уразливості	Сайти вендорів, www.cvedetails.com, exploit-db.com, 1337day.com	09.09 - 13.09

Продовження таблиці 2.3

	1	2	3
6.4	Аналіз можливості проведення спуфінгових атак на мережеві протоколи MAC, ARP, DHCP, IP, DNS, Netbios в локальному мережевому сегменті	Cain & Abel, Wireshark	16.09 - 18.09
6.5	Аналіз безпеки протоколів маршрутизації і резервування (RIP, OSPF, EIGRM, BGP, HSRP, VRRP та ін.)	Wireshark	16.09 - 18.09
6.6	Аналіз можливості обходу правил фільтрації і побудови бекдора в зовнішню мережу.	-	16.09 - 18.09
4 Фізична розвідка, сканування Wi-FI			
4.1	Фото-відеозйомка території об'єкта, вивчення контрольно-пропускної системи.	Фотоапарат з функцією відеозапису	16.09 – 18.0 9

Продовження таблиці 2.3

	1	2	3
4.2	Сканування WI-FI мереж	Устаткування для перехоплення - WI - FI модуль ALFA AWUS036NHR 2w + спрямована антена, коефіцієнт посилення 12 Дб.	16.09 - 18.09
7 Експлуатація вразливостей, проведення тестових спроб проникнення			
7.1	Верифікація потенційних вразливостей з високим і середнім рівнем критичності у зовнішньому периметрі мережі. Тестові спроби експлуатації і розвиток атак.	Публічні експлойти, і фреймворки, різний інструментарій для злому	05.09 - 27.09
7.2	Верифікація потенційних вразливостей з високим і середнім рівнем критичності у внутрішньому периметрі мережі. Тестові спроби експлуатації і розвиток атак.	Публічні експлойти, і фреймворки, різний інструментарій для злому	18.09 - 04.10

Продовження таблиці 2.3

	1	2	3
7.3	Підготовка і проведення фішингової розсилки	Email sender deluxe Сценарій 1: підміна вікна входу на portal bLA https: // port. bla. com Сценарій 2: розсилка вірусу	19.09 - 20.09
7.4	Підготовка і проведення обдзвону співробітників	-	23.09 - 24.09
7.5	Проведення спроби проникнення на територію компанії і в приміщення з обмеженим доступом	-	01.10 - 02.10
8 Аналіз ризиків та підготовка звіту			
8.1	Визначення цінності активів (аналіз збитку)	Інтерв'ю з представниками Замовника	03.10
8.2	Аналіз ризиків та складання моделі зловмисника	Аналіз ризиків за методологією IRAM	03.10 - 08.10
8.3	Підготовка та презентація фінального звіту	-	09.10

FOCA - є інструментом, який читає метадані з широкого діапазону документів та медіа-форматів. FOCA дістає відповідні імена користувачів, шляхи, версії програмного забезпечення, деталі принтера, і адреси електронної пошти. Це може все бути виконано без необхідності індивідуально завантаження файлів.

WHOIS – утиліта, яка дозволяє визначити кому належить домен або IP-адреса.

URLCrazy – утиліта для створення та тесту одруківок домену, варіації для виявлення й виконання одруківок, URL угін, фишинг та корпоративне шпигунство.

Httprint – цей веб-сервер є інструментом для «зняття відбитків пальців». Він спирається на характеристики веб-серверу, щоб виявити веб-сервери, не дивлячись на те, що вони, можливо , були очорнені зміною строк банер серверу, або плагінів, таких як mod_security або servermask. Також може бути використаний для виявлення веб-сумісних пристроїв, котрі не мають строки заголовку сервера, такі як бездротові точки доступу, маршрутизатори, комутатори, кабельні модеми тощо. Httprint використовує текстові строки підпису, а це дуже легко, додати підписи до бази даних підписів.

CMS (Content management system) - Система управління вмістом (контентом) - інформаційна система або комп'ютерна програма, яка використовується для забезпечення і організації спільного процесу створення, редагування і управління контентом (тобто вмістом) .

Основні функції CMS:

- Надання інструментів для створення вмісту, організація спільної роботи над вмістом;
- Управління вмістом: зберігання, контроль версій, дотримання режиму доступу, управління потоком документів і т. п.;
- Публікація вмісту;
- Представлення інформації у вигляді, зручному для навігації, пошуку;
- У системі управління вмістом можуть перебувати найрізноманітніші дані: документи, фільми, фотографії, номери телефонів, наукові дані і так далі.

Така система часто використовується для зберігання, управління, перегляду та публікації документації. Контроль версій є одним з основних її переваг, коли вміст змінюється групою осіб.

Nmap ("Network Mapper") - це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки. Вона була розроблена для швидкого сканування великих мереж, хоча прекрасно справляється і з одиничними цілями. Nmap використовує сірі IP пакети оригінальними способами, щоб визначити які хости доступні в мережі, які служби (назва програми і версію) вони пропонують, які операційні системи (і версії ОС) вони використовують, які типи пакетних фільтрів / брандмауерів використовуються і ще дюжини інших характеристик . У той час як Nmap зазвичай використовується для перевірки безпеки, багато мережеві і системні адміністратори знаходять її корисною для звичайних завдань, таких як контролювання структури мережі, управління розкладами запуску служб та облік часу роботи хоста або служби.

ICMP - Internet Control Message Protocol - протокол міжмережевих контрольованих повідомлень.

Maltego є спеціалізованим розвідувальним ПЗ, призначеним для збору інформації з різних баз даних, а також уявлення в зручному для розуміння форматі. Також дозволяє виявити основні зв'язки між шматками інформації і встановити раніше невідомі відносини між ними.

Dirbuster – Java-додаток, розроблений для брутфорсу директорій та імен файлів на веб/додатків-серверів.

Nessus - програма для автоматичного пошуку відомих вад у захисті інформаційних систем. Вона здатна виявити найпоширеніші види вразливостей, наприклад:

- Наявність вразливих версій служб або доменів:
- Помилки в конфігурації (наприклад, відсутність необхідності авторизації на SMTP-сервері);
- Наявність паролів за замовчуванням, порожніх, або слабких паролів;
- Програма має клієнт-серверну архітектуру, що сильно розширює можливості сканування.

Acunetix Web Vulnerability Scanner - автоматизує задачу контролю безпеки Web додатків і дозволяє виявити вразливі місця в захисті web-сайту до того, як їх виявить і використовує зловмисник.

Wireshark (раніше звався Ethereal) — програма для аналізу мережевих пакетів Ethernet і інших мереж (сніфер) з вільним вихідним кодом. Має графічний інтерфейс користувача. У червні 2006 року проєкт був перейменований на Wireshark через проблеми з торговою маркою. Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, проте Wireshark має графічний інтерфейс користувача і значно більше можливостей із сортування і фільтрації інформації.

Програма дозволяє користувачеві переглядати весь трафік, що проходить по мережі, в режимі реального часу, переводячи мережну карту в promiscuous mode. Wireshark — це програма, яка розпізнає структуру найрізноманітніших мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Оскільки для захоплення пакетів використовується pcap, існує можливість захоплення даних тільки з тих мереж, які підтримуються цією бібліотекою. Проте, Wireshark вміє працювати з безліччю форматів початкових даних, відповідно, можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.

2.3 Висновок

Як видно з описаного вище, тест на проникнення - це складна і об'ємна послуга, яка може показати поточну картину захищеності інформаційних систем. Результати проведення подібного тесту часто дивують керівництво компаній-замовників. З практики проведення тестів в Україні можна відзначити уразливості, пов'язані зі слабкою організацією в установці оновлень і латочок (patch management), проникнення всередину мережі через рідко використовувані сервіси, розташовані по сусідству з критичними бізнес додатками, несерйозне ставлення до питань обізнаності персоналу в питаннях

інформаційної безпеки, що дозволяє в 99% випадків успішно реалізувати атаки методами соціальної інженерії.

Нові вразливості в системах і технологіях виявляються практично щодня. Таким чином, захист інформації в компанії повинен стати постійним процесом, а не разовим заходом. Доброю практикою вважається проводити тести на проникнення як мінімум раз на рік, а в періоди між ними організувати процес управління уразливими (vulnerability management) шляхом закупівлі сканера вразливостей і періодичного самостійного сканування периметра мережі. Такий підхід забезпечить оптимальний захист від цілеспрямованих атак або з боку конкурентів або інших зацікавлених осіб, які мають певні ресурси (час, гроші, кваліфікованих фахівців і технології), порівнянних з вартістю самої інформації.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Розрахунок капітальних витрат

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

Фіксовані витрати на впровадження системи розраховуватимуться за формулою (3.1):

$$К = К_{пр} + К_{пз} + К_{ic}, \text{ грн.} \quad (3.1)$$

де $К_{пр}$ – вартість впровадження, грн;

$К_{пз}$– вартість додаткового програмного забезпечення, грн.;

$К_{ic}$– витрати інтеграцію розробленого Pentest. у вже існуючу систему, грн.

Розрахунок капітальних витрат буде проводитися на прикладі впровадження додаткового програмного забезпечення, призначеного для створення Pentest: автоматизований сканер вразливостей, програма перехвату проксі-серверів, підсистема аналізу вразливостей.

3.2.1 Розрахунок заробітної плати системного адміністратора

Впровадженням, налаштуванням та обслуговуванням додаткового програмного забезпечення, призначеного для створення Pentest, займається системний адміністратор.

Заробітна плата при простій часовій системі оплати праці визначається за формулою:

$$З = ТС* Ф , \quad (3.2)$$

де ТС – тарифна ставка привласненого робітникові кваліфікаційного розряду в одиницю часу (година, день, місяць), грн;

Ф – фактично відпрацьований час;

Почасова тарифна ставка системного адміністратора складає ТС = 200 грн/год.

Час на складання технічного завдання складає 20 год., на розробку структури Pentest складає 15 год., час на впровадження Pentest в існуючу інформаційну систему 10 год., час на розробку інструкцій користування Pentest 6 год. Отже, трудомісткість створення Pentest розробником складає:

$$t = 20 + 15 + 10 + 6 = 51 \text{ год.}$$

Витрати на розробку системи підтримки прийняття рішення складають:

$$К_{пр} = 200*51 = 10200 \text{ грн.}$$

3.2.2 Розрахунок капітальних витрат

В таблиці 3.1 наведені витрати на додаткове програмне забезпечення, необхідне для створення Pentest.

Таблиця 3.1 Вартість додаткового програмного забезпечення для створення Pentest

Найменування	Кількість, шт.	Ціна за 1 шт., грн.
1	2	3
Автоматизований сканер вразливостей Nessus;	1	16985
Програма перехвату проксі-серверів Burp;	1	13000
Підсистема аналізу вразливостей Accunetix.	1	18000
Загалом		47985

Отже, вартість додаткового програмного забезпечення складає:

$$К_{пз} = 47985 \text{ грн.}$$

Витрати на інтеграцію розробленої PENTEST В у вже існуючу корпоративну систему визначаються у 8 % до сумарної вартості обладнання та програмного забезпечення.

$$К_{ic} = 47985*0,08 = 3838,8 \text{ грн.}$$

Таким чином, капітальні витрати для створення PENTEST становлять:

$$К = 10200 + 47985 + 3838,8 = 62023,8 \text{ грн.}$$

3.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проєктування за визначений період (наприклад, рік), що виражені у грошовій формі.

Під «витратами на керування системою» маються на увазі витрати, пов'язані з керуванням й адмініструванням компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

- навчання адміністративного персоналу й кінцевих користувачів;
- амортизаційні відрахування від вартості обладнання та ПЗ;
- заробітна плата персоналу;
- навчальні курси й сертифікація обслуговуючого персоналу;
- технічне й організаційне адміністрування й сервіс.

До експлуатаційних витрат віднесено:

- заробітну плату співробітника системного адміністратора;
- витрати на ліцензію програмного забезпечення;
- Витрати на керування PENTEST.

Річні поточні витрати на функціонування системи заходів протидії загрозам інформації визначаються за формулою (3.3):

$$C = C_1 + C_2 + \ldots + C_n, \text{ грн,} \qquad (3.3)$$

де С – вартість підтримки заходу протидії загрозам інформації;

n – порядковий номер заходів протидії загрозам інформації.

Впровадженням, налаштуванням та обслуговуванням додаткового програмного забезпечення, призначеного для створення Pentest, займається системний адміністратор.

Заробітна плата системного адміністратора складає $З_{СА}$ = 200 грн/год.

Час на аналіз та зміну технічного завдання складає 1 год/тиждень:

С = ТС* Ф = 200*1*50 = 10000 грн.

Час на підтримку Pentest в існуючій інформаційній системі складає 1 год/тиждень, затрати:

С = ТС* Ф = 200*1*50 = 10000 грн.

Час на створення журналу обліку складає 1 год/тиждень:

С = ТС* Ф = 200*1*50 = 10000 грн.

Затрати на продовження ліцензії програмного забезпечення складають 47985 грн.

Значення загальних річних поточних витрат складає:

С = 10000 + 10000 + 10000 + 47985 = 77985 грн.

3.3 Оцінка можливого збитку від порушення інформаційної безпеки

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

3.4 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично неможливо. Природньо, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

–час простою внаслідок поломки, $t_п$ (в годинах), $t_п$ = 4 год;

–час відновлення після поломки, $t_в$ (в годинах), $t_в$ = 2 год;

–час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви}$ = 1 год;

–заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), Z_0 = 25000 грн.;

–заробітна плата співробітників, Z_c (грн. в місяць з податками), Z_c = 20000 грн.;

–кількість обслуговуючого персоналу, N_0, N_0 = 2;

–число співробітників, N_c, N_c = 20;

–прибуток , O (грн. на рік), O = 25000000 грн.;

–вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч}$ = 6000 грн.;

–число зламаного обладнання, I, I = 1;

–число поломок на рік, n, n = 8.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.10:

$$П_п = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_п, \text{ грн.}, \qquad (3.4)$$

де місячний фонд робочого часу складає 160 годин.

Підставивши вихідні дані отримаємо:

$П_п$ = (20*20000/160)*4 = 10000 грн.

Вартість відновлення зламаного обладнання розраховується за формулою 3.11:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.5)$$

де $П_{ви}$ – вартість повторного введення інформації (формула 3.12),

$П_{пв}$ – вартість відновлення обладнання (формула 3.13).

$$П_{ви} = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_{ви}, \text{ грн.} \quad (3.6)$$

$$П_{пв} = \frac{\sum Z_o}{\frac{N_o}{160}} \cdot t_в, \text{ грн.} \quad (3.7)$$

Отримаємо:

$П_{ВИ}$ = (20*20000/160)*2 = 5000 грн.

$П_{ПВ}$ = (2*25000/160)*3 = 937,5 грн.

Вартість заміни обладнання та запасних частин, виправлення помилок в системі, $П_{зч}$ (грн.)

$П_{зч}$ = 6000 грн.

Підставивши отримані результати в загальну формулу отримаємо:

$П_В$ = 5000 + 937,5 + 6000 = 11937,5 грн.

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.14 й 3.15 відповідно:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.8)$$

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), \text{ грн,} \quad (3.9)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить 2080 годин.

V = (25000000/2080)*(4+3+2) = 108173 грн.

U = 10000 + 11937,5 + 108173 = 130110,5 грн.

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складає (формула 3.16):

$$ОУ = \sum_{n}\sum_{I} U, \text{ грн.} \quad (3.10)$$

ОУ = 8 * 1 * 130110,5 = 1040884 грн.

3.5 Загальний ефект від впровадження моделі

Загальний ефект від впровадження моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії визначається за формулою 3.17 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, \text{ грн}, \quad (3.11)$$

де $ОУ$– загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн.;

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії, грн.

Таким чином, загальний ефект від впровадження становить:

E = 1040884* 0,5 – 77985 = 442457 грн.

3.6 Визначення та аналіз показників економічної ефективності моделі

Оцінка економічної ефективності моделі, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій *ROSI* (Return on Investment for Security) за формулою 3.18 та терміну окупності капітальних інвестицій T_o за формулою 3.19.

$$ROSI = \frac{E}{K}, \text{ частки одиниці}, \quad (3.12)$$

де E – загальний ефект від впровадження системи захисту, грн.;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Підставивши відповідні значення, маємо:

$$ROSI = 442457 / 62023,8 = 7,1$$

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.14)$$

Підставимо значення:

$$T_o = 1 / 7,1 = 0,14 \text{ року (1,7 місяці).}$$

3.7 Висновки до розділу

Основою для визначення витрат на створення систем інформаційної безпеки є концепція сукупної вартості володіння, яка включає наступні витрати: фіксовані (капітальні) вкладення і поточні.

Фіксовані (капітальні) витрати здійснюються на етапі створення системи підтримки прийняття рішення, поточні – на етапі її функціонування.

У ході виконання роботи було визначено вартість витрат на проєктування та впровадження тестування на проникнення в існуючу інформаційну систему. Капітальні витрати для створення PENTEST становлять 62023,8 грн.; загальні річні поточні витрати – 77985 грн.; загальний ефект від впровадження 442457 грн.; загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складає 1040884 грн.; загальний ефект від впровадження - 442457 грн.

Таким чином, доцільність й ефективність тестування на проникнення для управління інформаційної безпеки доведено, окупність складає 1,7 міс.

ВИСНОВКИ

При виконанні кваліфікаційної роботи проаналізовано процес активного аудиту інформаційної безпеки і розглянуто можливу модель розробки алгоритму проведення тестів на проникнення. Застосування тестів на проникнення для управління інформаційної безпеки є доцільним, адже дає змогу оброблювати значний обсяг слабко конструйованих даних.

Було розроблено детальний алгоритм тесту на проникнення.

Детальніше робота тесту на проникнення описана для складової процесу управління інформаційної безпеки – аналізу вразливостей інформаційної безпеки, а саме наведено рекомендації щодо проведення сканування системи інформаційної безпеки.

Проведення тестування на проникнення в процесі аудиту інформаційної безпеки є доцільними. Запропонована інструкція є ефективною та не суперечить законодавству України та іноземним нормативним документам, на основі яких вона була розроблена.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 *Cyber attacks rise from outside and inside corporations.* - Computer Security Institute;

2 *Global Security Survey: Virus Attack.* – InformationWeek;

3 *National Infrastructure Protection Center CyberNotes* - NIPC, # 15-99;

4 *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.* - General Accounting Office, Chapter Report, GAO / AIMD-96-84;

5 R. Power - *CSI Roundtable: Experts discuss present and future intrusion detection systems.* - Computer Security Journal, , № 1.;

6 T. Bass - *Intrusion Detection Systems & Multisensor Data Fusion: Creating Cyberspace Situational Awareness.* - Communicaions of the ACM, accepted for publication (draft);

7 T. Goan - *A Cop on the Beat: Collecting and Appraising Intrusion Evidence.* - Communicaions of the ACM., № 7, с. 46-52;

8 M. Stillerman, C. Marceau, M. Stillman - *Intrusion Detection for Distributed Applications.* - Communicaions of the ACM., № 7, с. 62-69;

9 Міжнародний стандарт ISO/IEC 27002:2005. Практичні правила управління інформаційною безпекою;

10 M. Crosbie, K. Price - *Intrusion Detection Systems.* - Purdue University, COAST Laboratory;

11 NIST SP800-115 Technical Guide to Information Security Testing and Assessment (Електрон. ресурс) / Спосіб доступу: URL: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf - заголовок з екрану;

12 ISACA Switzerland - Testing IT Systems Security With Tiger Teams (Електрон. ресурс) / Спосіб доступу: URL: http://www.isaca.org/Knowledge-Center/Pages/default.aspx - заголовок з екрану;

13 BSI - Study A Penetration Testing Model (Електрон. ресурс)/ Спосіб

доступу: URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile – заголовок з екрану;

14 PTES Technical Guidelines (Електрон. ресурс) / Спосіб доступу: URL: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines – заголовок з екрану.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1	39	
6	А4	Розділ 2	35	
7	А4	Розділ 3	9	
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	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація_Виблий.ppt

2 Кваліфікаційна робота_Виблий.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22з-1 Виблого С.Р. на тему: «Розробка алгоритму проведення тесту на проникнення при аудиті інформаційної безпеки підприємства»

Кваліфікаційна робота представлена пояснювальною запискою на 99 с., містить 8 рис., 6 табл., 4 додатка, 14 джерел.

Мета кваліфікаційної роботи: забезпечення рівня інформаційної безпеки шляхом розробки тестів на проникнення в процесі активного аудиту.

Об'єктом дослідження є аудит інформаційної безпеки.

В роботі проаналізовано систему інформаційної безпеки на підприємстві.

В спеціальній частині представлений алгоритм проведення тесту на проникнення в процесі аудиту інформаційної безпеки, а також розроблено алгоритм та рекомендації щодо вибору способів обробки вразливостей інформаційної безпеки.

В економічному розділі проведено розрахунок вартості розробки алгоритму тесту на проникнення у вже існуючу інформаційну систему та зроблено висновок щодо доцільності проведення тесту на проникнення.

Наукова новизна полягає в обґрунтуванні та створенні моделі алгоритму тесту на проникнення для процесу аудиту інформаційної безпеки.

В якості недоліків слід зазначити незначні відхилення від графіку проведення робіт та норм при оформленні пояснювальної записки.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Виблий С.Р. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доц. **Сафаров О.О.**