НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ННК "Інститут прикладного системного аналізу"
(повна назва інституту/факультету)

Кафедра системного проектування
(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри
_____ А.І.Петренко
(підпис) (ініціали, прізвище)

"___"_____2015 р.

Дипломна робота
На здобуття ступеня бакалавра

зі спеціальності 6.050101 Комп'ютерні науки
(код та назва спеціальності)

на тему: «Аналіз захищених Proxy-з'єднань»

Виконав: студент IV курсу, групи ДА-11
(шифр групи)

Казаченко Ольга Дмитрівна _____
(прізвище, ім'я, по батькові) (підпис)

Керівник доцент, к.т.н., Кірюша Б.А. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант охорона праці доцент, канд. біол. наук. Гусєв А.М. _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент _____ доцент, к.т.н., _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Нормоконтроль ст. викладач Бритов О.А. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студент _____
(підпис)

Київ – 2015

Національний технічний університет України
«Київський політехнічний інститут»

Факультет (інститут) ННК "Інститут прикладного системного аналізу"
(повна назва)

Кафедра Системного проектування
(повна назва)

Рівень вищої освіти – перший (бакалаврський)

Спеціальність 6.050101 Комп'ютерні науки
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ А.І.Петренко
(підпис) (ініціали, прізвище)
«___»_____2015 р.

ЗАВДАННЯ
на дипломну роботу студенту
Казаченко Ользі Дмитрівні
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз захищених Proxy-з'єднань

керівник роботи Кірюша Богдан Анатолійович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «02» квітня 2015 р. №30/1-ст

2. Строк подання студентом роботи 08.06.2015

3. Вихідні дані до роботи:

Практичне уявлення про реалізацію захищених Proxy у розподілених системах. Аналіз уразливостей систем без використання захищених проксі серверів та з їх використанням.

4. Зміст розрахунково-пояснювальної записки (перелік завдань, які потрібно розробити)

1. Дослідити особливості розподіленої системи та засоби реалізації механізмів захисті інформації в ній.
2. Розглянути технології, що використовуються для встановлення Proxy-з'єднань.

3. Протестувати систему захищених Proxy на уразливості, та зробити висновки про її надійність на основі отриманих даних.
4. Розглянути питання з охорони праці та безпеки у надзвичайних ситуаціях при використанні результатів дипломного проекту.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

1. Алгоритм авторизації – плакат.
2. Захищене з'єднання – плакат.
3. Структура Proxy – плакат.
4. Proxy- сервер - плакат.
5. Презентація у форматі Power Point.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	к.б.н., доц. Гусєв А.М.		
Основна частина	Кірюша Б.А., доцент		

7. Дата видачі завдання 01.02.2015

Календарний план

№ з/п	Назва етапів виконання дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Отримання завдання	01.02.2015	
2	Збір інформації	15.02.2015	
3	Аналіз вимог технічного завдання, підбір літератури, підбір тестів, формування плану експериментів	28.02.2015	
4	Підготовка теоретичної частини роботи	10.03.2015	
5	Розробка плану тестування	15.03.2015	
6	Підготовка графічного матеріалу	18.04.2015	
7	Тестування моделі	27.04.2015	
8	Оформлення дипломної роботи	31.05.2015	
9	Отримання допуску до захисту та подача роботи в ДЕК	08.06.2015	

Студент _____ О.Д, Казаченко
(підпис) (ініціали, прізвище)

Керівник роботи _____ Б.А. Кірюша
(підпис) (ініціали, прізвище)

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПЗ - Програмне забезпечення

САПР - Система автоматизованого проектування

URL - Uniform Resource Locator

HTML - HyperText Markup Language

IDL - Interface Definition Language

DNS - Domain Name System

OSI - Open Systems Interconnection Reference Model

RPC - Remote Procedure Call

TSB - Trusted Computing Base

DES - Data Encryption Standard

KDC - Key Distribution Center

ACL - Access Control List

SOCKS - SOCKet Secure

HTTP - HyperText Transfer Protocol

NAT - Network Address Translation

VPN - Virtual Private Network

SSH - Secure Shell

Зміст

ВСТУП

На сьогоднішній день гостро постає питання безпеки інформації при обміні даними через недовірене середовище – Інтернет. Тим не менш, розповсюдження Інтернету та активне використання online-серверів приймає масовий характер. Відправлення документів, спілкування чи здійснення фінансових операцій засобами Інтернету стає щоденною потребою. І кожен раз потрібно впевнитись, що, наприклад, дані про засоби оплати та ваш рахунок гарантовано не стануть відомими для всіх, окрім вас.

Вимоги до забезпечення контролю над доступом до інформації лише тих користувачів, що мають на це права, нажаль не висунуті на державному рівні. Але актуальності цього питання є беззаперечною, особливо у банківській сфері. Збереження контролю над доступом при банківських транзакціях та переведенні грошових коштів є головним питанням безпеки фінансової сфери в Інтернеті. На сьогодні досить розповсюджене керування власними рахунками сидячи вдома, але засоби доступу не завжди можуть гарантувати належну безпеку конфіденційній інформації.

Для забезпечення захисту інформації користувачів та попередження викрадення персональних даних потрібна ефективна система аутентифікації, щоб гарантувати надійність підтвердження особистості користувача.

Метою даної роботи є дослідження механізмів захисту в розподілених системах та аналіз прокси-з'єднань, як частини цієї системи. Для реалізації цієї мети було розглянуто структуру та механізм реалізації proxy авторизації та аналіз її надійсності в плані гарантування анонімності особистим даним. Також досліджені види та цілі proxy-серверів та їх доцільність у порівняні з іншими механізмами забезпечення анонімності. Останнім етапом є тестування існуючого захищеного proxy сервера за допомогою сканера уразливостей, та аналіз отриманих даних.

1 АНАЛІЗ РОЗПОДІЛЕНИХ СИСТЕМ ТА МЕХАНІЗМІВ ЇХ ЗАХИСТУ

1.1 ЗАГАЛЬНИЙ ОГЛЯД АРХІТЕКТУРИ РОЗПОДІЛЕНИХ СИСТЕМ

Розподілена система — це набір незалежних комп'ютерів, що представлені користувачам, як єдина об'єднана система. Мається на увазі, що всі машини в системі автономні, а користувачі вважать, що мають доступ до єдиної системи.

Розглянемо основні важливі характеристики розподілених систем. По-перше, від користувачів сховані відмінності між комп'ютерами та способи зв'язку між ними. По-друге, це спосіб за допомогою якого працюють користувачі та програми в розподілених системах, не враховуючи місця та час їх взаємодії.

Розподілені системи також повинні мати здатність до досить легкого розширення та масштабування. Наявність цієї характеристики напряму випливає з присутності в системі незалежних комп’ютерів, але, тим не менш, не пояснює принцип, за яким насправді відбувається об'єднання цих комп’ютерів в єдину систему. Розподілені системи, зазвичай, постійно існують, хоча при цьому абсолютно можливий тимчасовий вихід з ладу деяких її частин. Користувачі та програми не повинні усвідомлювати факт заміни чи додання нових частин для підтримки додаткових користувачів та програм.

Для того щоб було можливо підтримувати цілісне представлення різних комп’ютерів та мереж у вигляді єдиної системи, організація розподілених систем часто має додаткових рівень програмного забезпечення в своїй ієрархії. Він знаходиться між верхнім рівнем (користувачі та програми) та нижнім (складається з операційних систем). Така ієрархія

побудови розподіленої системи має назву middleware, тобто система проміжного рівня, що зображена на рисунку 1.1.

Рисунок 1.1 - Розподілена система проміжного рівня

Можливість створення розподіленої системи не означає доцільність цього. Розподілені системи мають змогу легко надавати користувачам доступ до ресурсів, не виявляючи факту, що вони розкидані по мережі й можуть бути відкритими та здатними до масштабування.

Основною метою при створенні розподіленої системи є забезпечення користувачам легкого доступу до віддалених ресурсів, включаючи спільне використання та регулювання цього процесу. До ресурсів відносимо принтери, комп'ютери, файли та дані, а також веб-сторінки та мережі. Можливості з'єднання користувачів та ресурсів призвело до полегшення обміну інформацією, що гарно простежується на прикладі Інтернету. Зв'язок через Інтернет дозволив географічно віддаленим групам людей працювати разом за допомогою систем групової роботи – програм, що дозволяють спільно редагувати дані, проводити телеконференції та інше.

З розповсюдженням спільного доступу до інформації все гостріше постає питання безпеки. На практиці захист від прослуховування ліній зв'язку є досить слабким. Також паролі та подібна важлива інформація

частіше пересилається незашифрованим текстом і зберігається на серверах з сумнівною безпекою.

1.1.1 ВЛАСТИВОСТІ РОЗПОДІЛЕНОЇ СИСТЕМИ

1.1.1.1 ПРОЗОРІСТЬ

Розподілена система передбачає приховання того факту, що процеси та ресурси фізично розподілені серед багатьох комп’ютерів. Представляючись користувачам у вигляді цілісної системи, вони мають назву – прозорі. Прозорість в розподілених системах може бути застосована до різних аспектів.

Прозорість доступу (access transparency) створена для приховання відмінностей в представленні даних і в способах доступу користувача до ресурсів. Наприклад, розподілена система може містити комп’ютери з різними операційними системами, кожна з яких має власні обмеження на спосіб представлення імен файлів. Така різниця в обмеженнях на представлення імен файлів, а також робота з ними, й повинна бути прихована від програм та користувачів.

Прозорість місцезнаходження (location transparency) використовується для приховання від користувача фізичного розміщення в системі ресурсу, що цікавить. Ім'я ресурсу відіграє важливу роль в цьому, а прозорість може бути досягнута шляхом присвоєння йому лише логічного імені, тобто такого, що не містить в собі закодованих даних про своє місцезнаходження, наприклад URL (Uniform Resource Locator). При цьому не буде й жодної інформації про тривалість чи зміну його місцезнаходження. Якщо зміна місцезнаходження ніяк не впливає на доступ до ресурсу, збережена прозорість переносу (migration transparency) розподіленої системи. Можлива навіть зміна місцезнаходження у момент використання користувачем ресурсу, так що програми нічого не помітять, підтримуючи прозорість зміни місцезнаходження (relocation transparency).

Важливе місце в розподілених системах надане реплікації, що дозволяє покращити доступність до ресурсу та підвищити продуктивність, розміщуючи копію ресурсу недалеко від місця, з якого до ресурсу здійснюється доступ. Прозорість реплікації (replication transparency) дозволяє приховати факт наявності декількох копій ресурсу, привласнюючи всім копіям однакове ім'я. Система з підтримкою прозорості реплікації має підтримувати й прозорість місцезнаходження. Тим самим забезпечується можливість звернення до копій не зазначаючи її фізичного місцезнаходження.

Спільний доступ до ресурсів в багатьох випадках забезпечується засобами кооперації, але є й випадки дійсно спільного доступу, коли два користувачі можуть зберігати свої файли на одному сервері чи працювати з одною таблицею в базі даних з спільним використанням. Така одночасна взаємодія з одним й тим самим ресурсом зберігається в таємниці від обох користувачів й реалізує прозорість паралельного доступу (concurrency transparency). При цьому цей ресурс зберігається в стані не протиріччя. Це забезпечується механізмом блокування, коли користувачі по черзі отримують виключні права на ресурс, або більш складним способам – транзакціями.

Прозорість відмов (failure transparency) означає, що користувач не попереджений про збій в роботі ресурсу та про її відновлення. Маскування відмов настільки складна, наскільки й необхідна частина розподіленої системи. Тяжкість полягає у виявленні різниці між непрацюючими ресурсами, та ресурсами з низькою швидкістю відгуку.

Прозорість збереження ресурсів (persistence transparency) необхідна для маскування реального (диск) чи віртуального (оперативна пам'ять) збереження ресурсів.

Досягнення прозорості в розподілених системах виправдано, але не повинно розглядатись в сукупності з іншими характеристиками системи й не впливати, наприклад, на її продуктивність.

1.1.1.2 ВІДКРИТІСТЬ

Відкрита розподілена система (open distributed system) – це система, що пропонує служби, виклик яких потребує стандартного синтаксису та семантики. Такі служби зазвичай визначаються через інтерфейси, що переважно описуються за допомогою мови визначення інтерфейсів (Interface Definition Language, IDL). Опис інтерфейсу на IDL стосується синтаксису служб, тобто, воно точно відображає імена доступних функцій, типи параметрів, виключні ситуації, що викликані службою та інше. Найскладніше описати те, що дана служба виконує, тобто семантику інтерфейсів.

За правильного опису, визначення інтерфейсу допускає можливість спільної роботи довільного процесу, що його потребує, з іншим процесом, що його надає. Визначення інтерфейсу також дозволяє двом незалежним групам створити абсолютно різні реалізації цього інтерфейсу для двох різних розподілених систем, які будуть працювати повністю однаково. Правильне визначення самодостатнє й нейтральне. Під самодостатнім мається на увазі, що в ньому є все необхідне для реалізації інтерфейсу, хоча переважно це не реалізується розробником повною мірою. Специфікація має носити нейтральний характер й не визначати зовнішній вигляд інтерфейсу. Самодостатність й нейтральність необхідні для забезпечення взаємодії та переносу. Здатність до взаємодії характеризує міру можливості двох реалізацій систем чи компонентів від різних розробників працювати разом, якщо вони відповідають одному стандарту. Портативність визначає можливість програми, що розроблена для однієї розподіленої системи, без змін виконуватись в іншій, при цьому реалізуючи ті ж самі інтерфейси.

Важливою характеристикою розподілених систем є гнучкість. Вона визначає легкість конфігурації системи, що складається з різних компонентів, додавання або заміни компонентів.

Таким чином відкрита розподілена система повинна мати здатність до розширення. Для побудови таких систем потрібна вірна організація цих систем у вигляді наборів невеликих та легко замінних компонентів. Для

цього повинні бути визначені як інтерфейси з якими працюють користувачі та програми (верхній рівень) так і інтерфейси внутрішніх модулів системи и опис їх взаємодії.

1.1.1.3 МАСШТАБУВАННЯ

Масштабування розподіленої системи, як одна з найважливіших задач у її проектуванні, може вимірюватись по трьом параметрам. По-перше, по відношенню до її розміру, тобто легкості підключення до неї нових ресурсів та користувачів. По-друге, географічно, тобто розмежованості користувачів та ресурсів у просторі. По-третє, в адміністративному плані, тобто наскільки вона легко керується при роботі в множині адміністративно незалежних організацій. Здатність системи підтримувати масштабованість впливає на її продуктивність.

Якщо постає питання необхідності масштабування системи, то виникає ряд проблем, що потребують вирішення. Так, при збільшені числа користувачів чи ресурсів зіштовхуємося з обмеженнями централізованих служб, даних та алгоритмів. Наприклад, багато служб реалізуються централізовано, передбачуючи наявність в розподіленій системі лише одного серверу, що працює на конкретній машині. Маючи таку схему побудови системи, при збільшенні числа користувачів, такий сервер стає слабким місцем. Навіть якщо фактична кількість ресурсів, з якими ми маємо справу, необмежена за потужністю обробки та зберігання даних, ресурси, пов’язані з цим сервером, врешті решт, себе вичерпають, обмежуючи наш ріст.

На жаль, повністю уникнути випадків з використанням єдиного серверу – неможливо. Іноді це просто необхідно і обумовлено потребою організації окремої служби для роботи з конфіденційними даними окремо на сервері, що буде знаходитись в добре захищеному приміщені, а також засобами спеціальних мережевих пристроїв відокремлюватись від інших частин розподіленої системи. Реплікація даних в такому випадку

виключається, як спосіб підвищення продуктивності, адже безпека та стійкість служби до атак є найголовнішою метою.

Централізація даних також перешкоджає масштабуванню, як і централізація служб. За таких умов навантаження на вхідних та вихідних лініях зв’язку єдиної бази даних призведе до перевантаження. Для розуміння, можна лише уявити як би здійснювався доступ до веб, якщо служба доменних імен (DNS) була б реалізована у вигляді однієї таблиці, а кожен запит на інтерпретацію URL передавався б на єдиний DNS-сервер.

В великих розподілених системах велика кількість повідомлень повинні передаватись великою кількістю каналів, а для обрання оптимального шляху потрібно мати повну інформацію про навантаження всіх машин та каналів зв’язку, й за алгоритмами теорії графів обчислити всі оптимальні маршрути. Потім ця інформація повинна бути розіслана по системі для покращення маршрутизації. Проблема в тому, що такий постійний кругообіг цієї інформації може призвести до перевантаження частини мережі повідомленнями. Фактично алгоритму, що реалізується способом зібрання інформації про стан системи на одну машину, обробляється там, а потім розсилає результати назад, слід уникати. Кращим варіантом є використання децентралізованих алгоритмів, що володіють такими рисами:

1. Жодна машина не містить повну інформацію про стан мережі;
2. Оптимальні рішення формуються машинами на основі локальних даних;
3. Збій однієї машини не впливає на роботу інших;
4. Немає необхідності в припущені існування єдиного часу.

Під останнім розуміється, що неможливо синхронізувати всі годинники у світі, тому алгоритми повинні працювати без жодної прив’язки до конкретного часу. Чим більша система тим більше розбіжностей виникає. Для локальної мережі можливо досягти похибки в синхронізації часу, якою можна знехтувати, але на жаль не в межах країни, чи декількох країн.

1.1.2 МОДЕЛЬ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ.

Для спрощення роботи з різними рівнями мережевих взаємодій Міжнародна організація по стандартам ISO розробила еталонну модель взаємодії відкритих систем – OSI (Open Systems Interconnection Reference Model). Модель передбачала взаємодію відкритих систем по стандартним правилам, що визначають формат, зміст та сенс повідомлень. Ці правила описані у протоколах. Всі передбачені взаємодії відбуваються на семи рівнях, показаних на рисунку 1.2.

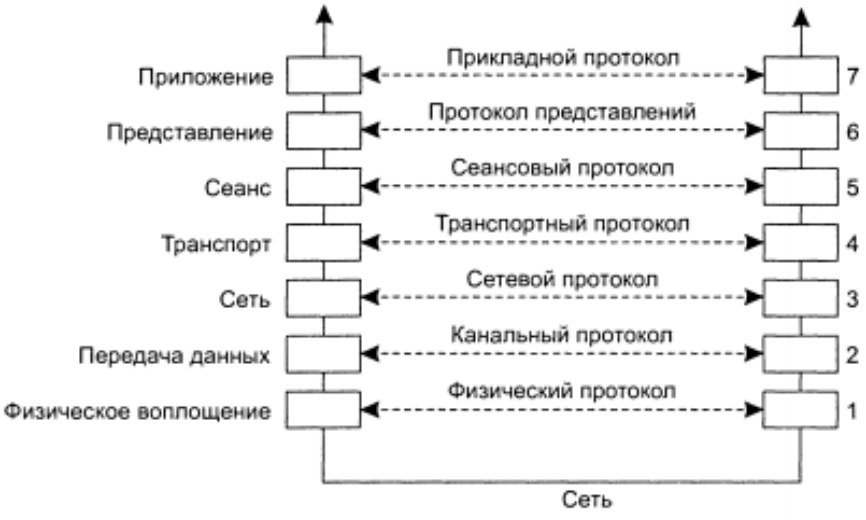


Рисунок 1.2 - Рівні моделі OSI.

Так повідомлення збирає інформацію про використані протоколи починаючи з верхнього рівня, а коли доходить до фізичного, виконується реальна передача, що показано на рисунку 1.3. Деякі рівні записують не лише заголовок в початок, але й завершення в кінець.

Рисунок 1.3 - Передача типового повідомлення

Фізичний рівень забезпечує стандартизацію електричних, механічних і сигнальних інтерфейсів. Відповідає лише за пересилання біт.

Канальний рівень вирішує питання знаходження та усунення виникаючих помилок. Він групує біти в кадр, додає контрольну суму і слідкує за їх вірною передачею.

Мережевий рівень забезпечує вибір маршрутизації, тобто найліпшого шляху для передачі даних.

Транспортний протокол гарантує потрібну міру надійності. Головною його задачею є знайти та усунути помилки в передачі даних, в часному випадку, організації повторної передачі пошкоджених чи загублених повідомлень. Перераховані протоколи складають базовий стек мережевих протоколів, й реалізують всі потрібні служби для побудови мережевих додатків.

Інші протоколи є протоколами верхнього рівня й зазвичай збираються до купи. Так, сеансовий рівень фактично розширює транспортний, відповідаючи за організацію сеансів зв’язку між різними робочими станціями. Представляючи засоби синхронізації, застосовується з метою підвищення надійності передачі інформації. Протоколи представлення, характеризують вид представлення даних, їх інтерпретацію, кодування та синтаксис для прикладного рівня, шифрування даних.

Прикладний рівень – набір різних протоколів, для забезпечення виконання прикладних задач. За їх участі відбувається доступ до розподілених ресурсів мережі.

В розподілених системах проміжного рівня виникає потреба в спеціальному наборі протоколів, які логічно відносяться до протоколів прикладного рівня, але містять багато протоколів загального призначення, тим самим формують новий рівень більш спеціалізованих додатків. Існує багато протоколів для підтримки служб проміжного рівня. Наприклад, до них

відносять різні методи аутентифікації, що не мають прив’язки до конкретних додатків. Протоколи авторизації, що визначають доступ процесів та користувачів тільки до ресурсів на яких вони мають право, також відносять до незалежного від додатків рівня. Комунікаційні протоколи проміжного рівня підтримують високо рівневі комунікаційні служби. Основні з яких це: віддалений виклик процедур, віддалене звернення до розподілених об’єктів, черг повідомлень та потоків даних.

Такий підхід приводить нас к трохи видозміненій організації рівнів в моделі OSI (Рисунок 1.4).

Рисунок 1.4 - Модель мережевої взаємодії

Основою множини розподілених систем являється явний обмін повідомленнями між процесами, що забезпечується комунікаційними службами, однак процедури їх відправки та прийому не приховують взаємодію, яка необхідна для забезпечення прозорості доступу.

Вирішенням цього став новий метод взаємодії, що дозволив програмам викликати процедури на інших комп’ютерах. Таким чином процес на машині А викликає процедуру на машині Б, при чому даний процес на машині А призупиняє свою роботу, а виконання викликаної процедури відбувається на машині Б. Вхідні дані можуть бути передані процедурі через параметри з першої машини, а потім повернені на неї результати виконання. Така взаємодія повністю прихована від користувача й називається віддалений

виклик процедур (Remote Procedure Call, RPC). Ця технологія є широко розповсюдженою і виступає базою для багатьох розподілених систем.

1.2 ОРГАНІЗАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ

Системи захисту в розподілених системах можна поділити на дві незалежні частини. По-перше, це зв'язок між користувачами чи процесами на віддалених машинах. Спосіб гарантування надійності в такому випадку – захищений канал. По-друге, це авторизація, що гарантує надання доступу до ресурсів розподіленої системи тільки тим процесам, що мають на це право.

Під поняттям надійності, мається на увазі доступність, безвідмовність та безпека системи, що зберігає при цьому цілісність та конфіденційність. Конфіденційність – це стан системи, коли доступ до інформації в ній обмежується певним колом довірених осіб. Цілісність – характеристика, що показує: можливість змін до системи може бути зроблена лише авторизованими користувачами.

Захист інформації передбачає уникнення перехвату, переривань, модифікації та підробок. Перехват – можливість неавторизованому суб’єкту отримати доступ к службам чи даним. Переривання – ситуація, в якій служби та дані можуть стати недоступними чи непридатними для використання. Модифікації – зміна даних в системі неавторизованими суб’єктами. При підробці створюються додаткові дані неможливі в нормальній системі.

Правила захисту реалізуються в механізмах захисту і визначають вид допустимих та недопустимих дій для системи (користувачів, служб, даних, машин та інше). До механізмів захисту відносять:

1. Шифрування – трансформація даних в стан, що не може бути зрозумілим стороннім. Це засіб реалізації конфіденційності.
2. Аутентифікація - це процес перевірки та підтвердження ідентичності суб'єкта чи об'єкта. В контексті інформаційної безпеки під процесом аутинтифікації розуміємо – єдиний метод, що використовується для

управління доступом до облікового запису користувача та його особистим даним. Передбачається, що користувачем в інформаційній системі повинні бути пред'явлені особисті дійсні ідентифікаційні дані, що супроводжуються мінімально одним аутентифікуючим фактором для підтвердження дійсності.

3. Авторизація – надання аутентифікованому користувачу прав згідно з його рівнем доступу.
4. Аудит – контроль дій користувача.

Для організації захисту потрібно визначити кількість рівнів механізмів захисту. Рівень стосується логічної організації системи. Структурна модель була розглянута в першому розділі, і зображена на рисунку 1.4.

Рисунок 1.4 - Логічна багаторівнева організація.

За зображенням служби загального призначення є відділеними від комунікаційних, що має значення для розподілення по рівням механізмів захисту та уявлення про довіреність. Рівень на якому розміщені системи захисту, залежать від довіри користувача до служб цього рівня. В розподілених системах механізми захисту зазвичай відносять до проміжного рівня, де реалізована локальна служба захисту RPC. Служби захисту, що розміщенні на проміжному рівні, викликають довіру, якщо служби на які вони спираються також захищені. Такий взаємозв’язок передбачає наявність набору всіх механізмів захисту розподіленої системи – довіреної обчислювальної бази (Trusted Computing Base, TSB). TSB – може включати захист локальних операційних систем.

Криптографія відіграє значну роль в захисті розподілених систем. Шифрування та розшифрування повідомлень забезпечується різними криптографічними методами. Криптосистеми можуть бути симетричними, тобто використовувати для шифрування та дешифрації один ключ, та асиметричними, що використовують різні ключі та створюють унікальну пару. Найрозповсюдженіші криптосистеми це: симетрична Data Encryption Standard (DES) та асиметрична з відкритим ключем — RSA.

1.2.1 АВТОРИЗАЦІЯ

Процес авторизації в розподілених системах пов'язаний з аутентифікацією користувача, та, після підтвердження його ідентичності, надання йому прав доступу. Аутентифікація нероздільна з цілісністю повідомлення, тобто впевненість в визначеності особи, яка відправила повідомлення, й отриманні вихідної версії повідомлення, написаної цією особою.

Розглянемо декілька протоколів аутентифікації:

1. Аутентифікація на основі таємного ключа;
2. Аутентифікація з використанням KDC (Key Distribution Center);
3. Аутентифікація на основі криптосистеми з відкрити ключем.

Після процесу аутентифікації користувачу надаються права на доступ до інформаційних ресурсів. Таким чином при запиті клієнта до конкретного методу об’єкта, виконаний він буде лише у випадку коли клієнт володіє достатніми для такої взаємодії правами доступу.

Підтвердження цих прав називається контролем доступу, а їх видача відбувається службою авторизації. Модель контролю доступу складається з суб'єктів, які власне відправляють запит на доступ, та об’єктів, доступ до яких бажають отримати.(Рисунок 1.5).

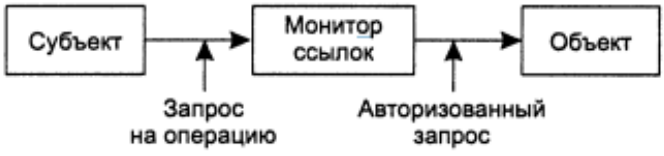


Рисунок 1.5 - Модель контролю доступу.

Одною з найважливіших властивостей об’єкту є приховання його внутрішньої структури під строго визначеним інтерфейсом. Об'єкт здатний інкапсулювати дані, що мають назву стани (state), та операції над цими даними - методи (methods). Єдиний правильний засіб доступу до об’єкту являється використання його методів, до яких отримуємо доступ через інтерфейс цього об’єкту. Захист часто надається монітором посилань, що записує можливі дії суб’єктів, і вирішує надавати чи ні доступ на виконання конкретної операції. Монітор викликається при будь-яких зверненнях до об’єкту і також повинен мати належний захист.

Контроль доступу може бути забезпечений матрицею, що містить відповідності методів та даних об’єкту суб’єктам, які мають на них права. Фізична реалізація такого принципу здійснюється шляхом її розбиття на списки контролю доступу – ACL. Списки розподіляються по об’єктам, та містять права доступу суб’єктів до своїх методів. Менш розповсюджений шлях реалізації матриці – розбиття її на мандати для кожного з об’єктів та закріплення за суб’єктами. Відсутність об’єкту мандата означає відсутність доступу до нього.

1.2.2 ДЕЛЕГУВАННЯ

Делегувати права доступу – означає можливість передавати права від одного процесу до іншого. Такий засіб – важливий елемент реалізації захисту розподілених систем і дозволяє розділити роботу між кількома процесами не шкодячи безпеці ресурсів. Таким чином розподілені системи можуть запускатись навіть в різних адміністративних доменах. Це також вирішує проблеми масштабованості та продуктивності системи, шляхом забезпечення більш швидкого доступу до даних.

Існує декілька способів забезпечення механізму делегування. Традиційно він реалізується за рахунок використання proxy. Серед інших

можливих варіантів: логіка монотонного та немонотонного делегування та з використанням агентів безпеки.

1.3 ВИСНОВОК

Забезпечення захисту в розподілених системах відіграє дуже важливу роль. Користувачам та розробникам повинні надаватись механізми, що реалізують різноманітні правила захисту. Розподілені системами повинні мати засоби організації захищених каналів зв’язку між процесами. Цей канал забезпечує засоби аутентифікації сторін і захищає повідомлення від фальсифікацій. Важливо визначитись буде використана симетрична криптосистема чи її поєднанням з відкритим ключем, що використовується для поширення сеансових ключів.

Після аутентифікації процесу завжди повинен відбуватись контроль доступу. Для надійності роботи розподілених систем повині бути надані засоби управління захистом. Вони повинні забезпечувати управління ключами та авторизацією.

2 ВИКОРИСТАННЯ PROXY-З'ЄДНАНЬ

2.1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Proxy, в контексті захисту комп'ютерних систем, являє собою маркер, який дозволяє оперувати з правами та привілеями їх власника, який надає маркер. Повинна бути можливість впевнитись, що proxy був наданий суб'єктом який він називає. Це проблема аутентифікації. Насправді суб'єкт з атрибутами прав доступу, що потребує спочатку аутентифікацію для себе, може надати маркер іншому суб'єкту просто передаючи ці атрибути доступу.

Реалізація proxy тягне таким чином за собою низку певних недоліків. По-перше, використати proxy може будь-хто, хто його контролює. Це може й не бути проблемою, але в багатьох випадках повинна бути змога вказати суб'єкти, які можуть діяти від його імені. По-друге, користувач, що забезпечений proxy-маркером, може виконувати всі дії, доступні суб'єкту, який його надав, на будь-якому сервері з оригіналами прав доступу.

Обмежені proxy - це proxy властивості яких залежать від їх використання. Суб'єкт, який володіє обліковими даними для авторизації чи аутентифікації може створити обмежені proxy, новий набір прав доступу, який буде більш обмеженим ніж оригінальні права. При цьому усунути обмеження неможливо. Сервер, якому будуть надані обмежені proxy, повинен мати змогу впевнитись, що обмеження не були підроблені. Серед обмежень, які часто зазначені є такі, що proxy можуть бути використані лише установленими суб'єктами, чи такі, що обмежують операції, які можна виконати.

Коли суб'єкт видає обмежені proxy іншому, той стає уповноваженим виконувати всі операції, для яких перший суб'єкт є авторизованим на сервері

чи серверах, яким відповідають proxy з урахуванням будь-яких обмежень, записаних у proxy.

Енд-сервер – це сервер якому повинні бути пред`явлені proxy для виконання операцій.

Обмежені proxy складаються з двох частин (рисунок 2.1):

1. Сертифікат, підписаний особою, яка надає права доступу, з перерахуванням всіх обмежень та створенням шифрувального ключа для представлення його серверу, який повинен буде підтвердити, що proxy був належним чином виданий його пред’явнику.

2. Proxy-ключ, ключ шифрування, що відповідає ключу вбудованому в сертифікат, що буде використаний пред’явником для підтвердження права на володіння proxy-маркером.

$$\text{Certificate: } [restrictions, K_{proxy}]_{grantor}$$
$$\text{Proxy-key: } K_{proxy}$$

Рисунок 2.1 - Структура обмежених proxy

В квадратних дужках визначається сигнатура, суб'єктом, який зазначений в індексі або під окремим ключем шифрування. Коли обмежені proxy передаються від власника, що надає їх, до суб’єкту, що їх отримує, повинна бути забезпечена підтримка для захисту proxy-ключа від виявлення.

Є два класи proxy: proxy на пред'явника і делеговані proxy. Proxy на пред'явника може бути використаний ким завгодно. Делеговані proxy можуть бути використані тільки суб’єктом, ім'я якого в списку делегатів (закодованого як обмеження), або кимось з відповідними додатковими proxy, наданими від імені одного з суб`єктів у списку.

Щоб представити proxy на пред'явника енд-серверу для виконання операцій, суб`єкт, що отримує права, відправляє сертифікат до сервера і використовує proxy-ключ, щоб взяти участь в обміні аутентифікації з енд-

сервером, використовуючи основний механізм аутентифікації. Зазвичай цей обмін передбачає відправку завіреної або зашифрованої тимчасової мітки або виклику сервера, доводячи володіння proxy-ключем.

Щоб уявити делеговані proxy, суб`єкт, що отримує права, відсилає сертифікат енд-серверу та потім авторизується під власною ідентичністю. Енд-сервер перевіряє сертифікат, щоб впевнитись, що клієнт потрапив до списку делегатів визначеного за допомогою proxy.

2.2 PROXY АВТОРИЗАЦІЯ

Обмежені proxy забезпечують засіб для реалізації широкого спектру механізмів авторизації в розподілених системах. На рисунку 2.2 показано взаємозв'язок механізмів в обмежених proxy та інфраструктури аутентифікації, від яких вони залежать.

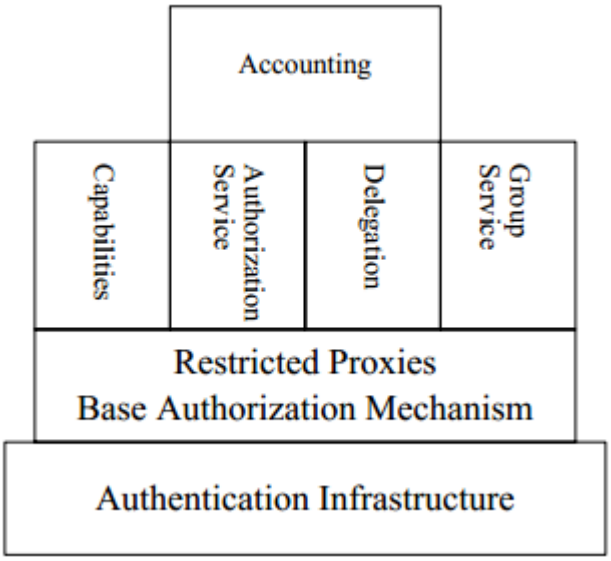


Рисунок 2.2 - Зв'язок proxy та аутентифікації

Можливості (те, що надають proxy) авторизації можуть бути розглянуті, як proxy на пред`явника, які є обмеженими в можливості виконання операцій та доступу до об`єктів. Обмеження не накладаються на суб`єкта, що отримує права, і є вільними в передачі можливостей іншим. При зверненні до енд-серверу, права суб`єкта, який надає права (обмежені), доступні пред`явнику.

Наприклад, щоб створити можливість прочитання файлу, користувач, що має права на це, відправляє серверу, що містить даний файл, запит на створення обмежених proxy з дозволом лише на прочитання даного файлу по його імені. Ці можливості передаються іншим, а ті в свою чергу, зможуть поділитись ними далі. Для використання можливості, вони мають бути пред'явлені енд-серверу в додаток до облікових даних суб'єкту. Запит, в межах наданих можливостей, виконується від прав суб'єкта, який надав proxy.

Є деякі відмінності між традиційними можливостями та описаними вище:

1. Суб'єкт не надає енд-серверу весь обмежений proxy. Він відправляє лише сертифікат, та підтверджує права приймаючи участь в авторизації використовуючи proxy-ключ. Так немає сенсу в прослуховуванні мережі на представлення користувачами своїх можливостей в ній.
2. Можливості втілюють в собі обмежене уособлення суб'єкта, який надав їх, не забезпечуючи прямий доступ до названого об'єкту. Так можливість може бути усунена шляхом зміни прав доступу, суб'єктом, який їх надав. Це вплине на всі забезпечені цим суб'єктом можливості та не змінить надані йому іншими. Відмінностей не буде, якщо суб'єкт, доступ якого передбачається, є власником об'єкту.
3. Багато систем аутентифікації забезпечують можливості лише тимчасово. Необмежені можливості реалізуються встановленням часу закінчення їх дії на достатньо далекий час в майбутньому.

2.2.1 СЕРВЕР АВТОРИЗАЦІЇ

Сервер авторизації, що надає proxy, отримуючи запит від авторизованого користувача, забезпечує його можливістю діяти від імені

сервера для підтвердження прав на об’єкт. Обмеження визначаються даними бази серверу.

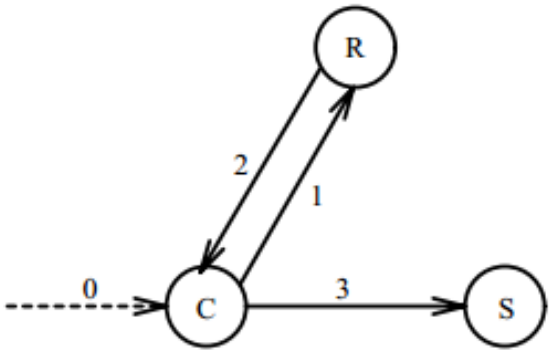


Рисунок 2.3 - Протокол авторизації

На рисунку 2.3 показано процес авторизації клієнта(C) на сервері(R) для отримання доступу до енд-серверу(S). Запит на авторизацію використовує основний протокол авторизації. В повідомленні 2 сервером надається сертифікат та proxy-ключ, для безпеки зашифрований криптографічним методом з використання сеансового ключа, створеного при відправленні повідомлення 1. Повідомлення 0 містить дані про повноваження, потрібні енд-серверу. Ця інформація – частина протоколу програми, витягнутого з імені сервера, чи отриманого безпосередньо від енд-серверу.

Енд-сервер бажаючи використовувати сервіси серверу авторизації, забезпечує між ними максимально прямий доступ.

2.2.2 ГРУПА СЕРВЕРІВ

Група серверів реалізована з використанням обмежених proxy надає proxy, які делегують право відстоювати членство в певній групі. Протокол такий же, як на рисунку 3.3; авторизована операція затвердження членства в групах.

Група серверів може обслуговувати більше однієї групи. Їх імена унікальні лише для конкретної групи серверів, а глобальні складаються з додаванням імені групи серверів.

Ім`я групи повинно з`являтись всюди в базі авторизації, де з`являється ім`я суб'єкту з цієї групи. Клієнт отримує груповий proxy й при відправлені запиту представляє його для підтвердження прав. Процес авторизації відбувається так само, як описано в 2.2.1.

2.2.3 КАСКАДНА АВТОРИЗАЦІЯ

Обмежені proxy мають схожі можливості з каскадним механізмом виконання операцій, учасники яких не довіряють один одному. Проходячи через проміжний сервер, що надав proxy, до підлеглого застосовуються додаткові обмеження. Вони додаються затвердженням нового proxy з оригінальним proxy-ключем. Новий proxy визначає додаткові обмеження та новий proxy-ключ. Сертифікати обох proxy надаються підлеглому серверу, але proxy-ключ лише кінцевому у ланцюгу. Рисунок 2.4 показує ланцюг proxy створений підлеглим сервером.

$$\begin{aligned}&\text{Certificate: } [restrictions1, K_{proxy1}]_{grantor}\\&\text{Certificate: } [restrictions2, K_{proxy2}]K_{proxy1}\\&\text{Certificate: } [restrictions3, K_{proxy3}]K_{proxy2}\\&\text{Proxy-key: } K_{proxy3}\end{aligned}$$

Рисунок 2.4 – Каскад proxy

Для делегованих proxy каскадна авторизація трохи інша. Для доступу до підлеглого серверу, проміжний сервер забезпечує його сертифікатом оригінального proxy.

Тому що проміжний сервер явно названий в оригінальному proxy, він також надає підлеглому новий proxy дозволяючи йому діяти в якості проміжного сервера з метою виконання початкового proxy. Замість підписання нового proxy з proxy-ключем від початкового proxy, він буде підписаний безпосередньо проміжним сервером.

2.2.4 МОЖЛИВОСТІ ДЛЯ ACL

Базуючи авторизацію на proxy-моделі, сервери додатків можуть легко комбінувати переваги листів контролю доступу і механізми авторизації на основі забезпечених proxy можливостей. Сервери додатків можуть бути розроблені для авторизації на основі локального списку контролю доступу.

Там, де вимагається підхід оснований на можливостях, що надають proxy, ACL повинен містити єдине ім'я входу суб'єкта, який має дозвіл на надання можливостей для серверних операцій.

Щоб, при необхідності, передати функцію авторизації до центру управління авторизацією або до групи серверів, ім`я авторизації чи групи серверів має бути додане до локального листа контролю доступу. Якщо досягнута локальна автономія, ім`я локального користувача в пару з ім`ям серверу авторизації буде занесене прямо до ACL. З моменту використання таких самих ACL абстракцій до серверу авторизації як до інших серверів, ACL записи можуть використовувати лист пов`язаних обмежень. На сервері авторизації, поле обмежень узгоджених ACL записів може бути скопійоване в відповідне поле нового proxy. Це додатково до обмежень перенесених з всяких proxy представлених серверу чи накладених ним самотужки.

Підтримуючи сполучення ідентифікаторів суб`єкту в ACL записах, стає можливим вимагати змогу деяких суб`єктів для конкретних операцій. Серед іншого, така функція дозволяє обумовлювати потребу конкретних операцій та розділення прав для повноважень хостів та користувачів, щоб користувач не міг діяти один. Авторизація основана на використанні proxy, дозволяє користувачам отримувати proxy на конкретну операцію більше ніж одному суб`єкту , залучаючи механізм підтвердження згоди користувача.

2.2.5 КРИПТОГРАФІЯ ПУБЛІЧНОГО КЛЮЧА

Сертифікат для публічного proxy-ключа містить proxy ключ наданий власником прав, час існування proxy та обмеження на його використання. Proxy-ключ є відкритим ключем з пари приватного/публічного ключа. Proxy-

ключ, наданий отримувачу – другий ключ з цієї пари. Всі поля підписані шляхом їх шифрування закритим ключем суб`єкта, що надає права.
На рисунку 2.5 показано таку генерацію proxy. Підписані proxy додатково мають тег власника для підтвердження коректності proxy та вибраного ключа.

$$\text{Certificate: } \{restrictions, K_{proxy}\}K^{-1}_{grantor}$$
$$\text{Proxy-key: } K^{-1}_{proxy}$$

Рисунок 2.5 - Відкритий ключ обмеженого proxy

Якщо система аутентифікації є чисто з відкритим ключем, алгоритм цифрового підпису з відкритим ключем може бути використаний замість системи шифрування, а крок шифрування буде замінений ущільненням сертифікату криптографічною контрольною сумою. Якщо використовується гібридна система аутентифікації, де наступні ключі беруться з звичайної криптосистеми, то proxy-ключ згенерований суб`єктом, що надає права, і повинен бути додатково зашифрований в публічному ключі енд-сервера, щоб захистити його від розкриття.

Коли пред`явник надає proxy енд-серверу, той дешифрує його використовуючи відкритий ключ суб`єкту, який його надав, підтверджує аутентичність proxy, приймає додаткову аутентифікацію власника прав (або персональну аутентифікацію для делегованих proxy або доказ того, що він знає proxy-ключ для proxy на пред`явника), перевіряє обмеження, і якщо все вірно виконує запитану операцію.

2.3 ЗВОРОТНІ PROXY-СЕРВЕРА

Традиційно, розміщення proxy-сервера базувалось на принципі: якомога ближче до користувача. Адміністратори конфігурували proxy-сервери для локальних мереж або користувачів невеликих організацій. У міру зростання популярності Web ряд Web-сайтів почав притягувати до себе

велику кількість користувачів. Щоб зменшити навантаження на сервери, proxy-сервери довелося розміщувати ближче до вихідних серверів. Такі proxy-сервери і отримали назву зворотних proxy-серверів, оскільки вони розташовувалися на іншому кінці ланцюжка запит-відповідь в порівнянні з традиційними proxy-серверами, розташованими ближче до користувача. Іншою причиною, з якої proxy-сервери стали розміщувати перед вихідним сервером, стало бажання зробити вихідні сервери «невидимими» для вхідних запитів. Зворотні proxy-сервери захищають вихідний сервер від прямих атак ззовні.

Проміжний компонент перед вихідними серверами може також надати допомогу в розподілі навантаження між групою серверів, обслуговуючих активно відвідуваний сайт. Proxy-сервер в цьому випадку переадресує запити на інші комп'ютери. Зворотний proxy-сервер представляється клієнту як вихідний сервер й діє як зовнішній інтерфейс для одного або кількох вихідних серверів, які можуть знаходитися за мережевим екраном. Клієнтський запит передається зворотному proxy-серверу, який пересилає його вихідного сервера. Зворотний proxy-сервер може також мати кеш. При пересиланні запиту зворотний proxy-сервер діє як тунель; тобто біти, передані в обох напрямках, залишаються без змін. Ззовні можна побачити лише одну IP-адресу - зворотного proxy-сервера.

Зауважимо, що хоча термін «зворотний proxy-сервер» став досить популярним, насправді необхідності в застосуванні окремого терміна немає. З точки зору клієнта він взаємодіє з вихідним сервером. Зворотний proxy-сервер є лише шлюзом, а взаємодія між зворотнім proxy-сервером і внутрішнім вихідним сервером (серверами) приховано від клієнта. Фактично зворотній proxy-сервер може не використовувати HTTP для взаємодії з вихідним сервером (серверами), що знаходяться позаду нього. Для зворотніх proxy-серверів в даний час використовується і новий термін - сервер-заступник.

2.4 HTTP PROXY ТА SOCKS-PROXY СЕРВЕРА

HTTP-proxy є самим широко поширеним в інтернеті. Додаток створено спеціально для роботи через браузери та інші затребувані широкою користувальницькою аудиторією програми, що працюють на протоколі HTTP.

HTTP-proxy має ряд корисних функцій:

1. Збереження переданих з інтернету файлів на диску proxy. Ця функція називається кешування і дозволяє істотно економити трафік.
2. Обмеження доступу до ресурсів. За допомогою даної опції створюється чорний список, тим самим, обмежується доступ користувачів до потенційно небезпечних інтерент-ресурсів.
3. Оптимізація ресурсу запитуваної браузером. Таким чином, користувач позбавляється від безлічі ненависних рекламних банерів понижуючих швидкість з'єднання.
4. Обмеження швидкості роботи для конкретних користувачів.
5. Робочий журнал. З його допомогою легко порахувати витрачений трафік і дізнатися частоту відвідуваності цікавлячого вас ресурсу.
6. Маршрутизація запитів дозволяє виробляти з'єднання з сайтами частково на пряму і частково через інші proxy. Робиться це для

HTTP-proxy-сервери, які приховують ip-адресу клієнта, називають анонімними. Такі сервери поділяються на види, ділення це вельми умовно, але, тим не менше, існують:

1. Прості анонімні proxy (anonymous). Ці сервери не приховують факту використання http-proxy, проте вони підміняють ip-адресу клієнта на свій.
2. Елітні анонімні (high anonymous / elite). Такі сервери ще приховують і сам факт використання http-proxy.
3. регулювання вартості і швидкості трафіку.

SOCKS-proxy-сервери. SOCKS — мережевий протокол, який дозволяє кліент-серверним додаткам прозоро використовувати сервіси за міжмережевими екранами (фаєрволами). SOCKS — це скорочення від «SOCKet Secure». Кліенти за міжмережевим екраном, що потребують доступ до зовнішніх серверів, замість цього можуть з'єднуватися з SOCKS proxy-сервером. Такий proxy-сервер контролює права клієнта для доступу до зовнішніх ресурсів і передає запит до сервера. SOCKS може використовуватися і протилежним способом, дозволяючи зовнішнім клієнтам з'єднуватися з серверами за міжмережевим екраном (брандмауером).

На відміну від HTTP proxy-серверів, SOCKS передає всі дані від кліента, нічого не додаючи від себе, тобто з точки зору кінцевого сервера, SOCKS proxy є звичайним клієнтом. SOCKS більш універсальний - не залежить від конкретних протоколів рівня додатків (7-го рівня моделі OSI) і базується на стандарті TCP/IP - протоколі 4-го рівня. Зате HTTP proxy кешує дані і може більш ретельно фільтрувати вміст переданих даних.

2.5 АНОНІМНІ PROXY

Відкритий proxy-сервер - proxy-сервер, що обробляє запити від будь-яких IP-адрес в Інтернеті. На відміну від звичайних proxy-серверів, якими користується обмежена кількість довірених осіб (зазвичай в зоні відповідальності власника proxy-сервера - наприклад, в локальній мережі), відкритий proxy-сервер дозволяє практично кожному вузлу мережі звертатися через себе до інших вузлів мережі.

При цьому, коли говорять про відкриті proxy-сервери, то найчастіше мають на увазі анонімні відкриті proxy-сервери, які приховують реальні IP-адреси клієнтів і тим самим надають можливість анонімно користуватися послугами мережі Інтернет (відвідувати сайти, брати участь у форумах, чатах, і т. д.). Це представляє деяку проблему, оскільки подібна анонімність може

дозволити безкарно порушувати закон і умови надання послуг в Мережі. З іншого боку, в недемократичних країнах анонімні proxy-сервери є однією з небагатьох можливостей вираження своєї думки, нехай і за своєрідною ширмою.

Proxy-сервер може бути зроблений відкритим (загальнодоступним) з волі власника сервера або в результаті неправильної конфігурації звичайного proxy-сервера (помилка при перевірці приналежності користувача, в налаштуванні «слухача» інтерфейсу, у списку трансльованих портів в NAT / PAT).

У разі різниці в ціні трафіку в різних мережах, відкритий proxy-сервер, що знаходиться у «своїй» мережі, може використовуватися для отримання більш дорогого трафіку з «чужої» мережі. Так, наприклад, багато російські користувачі, яким на роботі заборонений доступ до іноземних сайтів, можуть все-таки отримати такий доступ через відкритий proxy-сервер. Крім того, відкритий proxy-сервер може мати власний кеш, який прискорює доставку мережевих ресурсів клієнта.

Анонімні відкриті proxy-сервери можуть використовуватися для забезпечення (часткової) анонімності в Інтернеті, так як приховують IP-адресу користувача, направляючи всі запити користувачів від своєї адреси. При цьому сам proxy-сервер може вести протоколи (так звані «логи») звернень.

Відкриті proxy, як правило, високу швидкість передачі даних не забезпечують - ними користуються, зазвичай, для вчинення якоїсь конкретної операції, коли важлива не швидкість, а сам факт вчинення дії

2.6 VPN/SSH У ПОРІВНЯНІ З PROXY

2.6.1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА VPN/SSH

VPN, незважаючи на деякі відмінності, схожий за основним принципом на SSH-тунелі, тому розглянемо їх одночасно. Схема роботи VPN показана на рисунку 2.6.

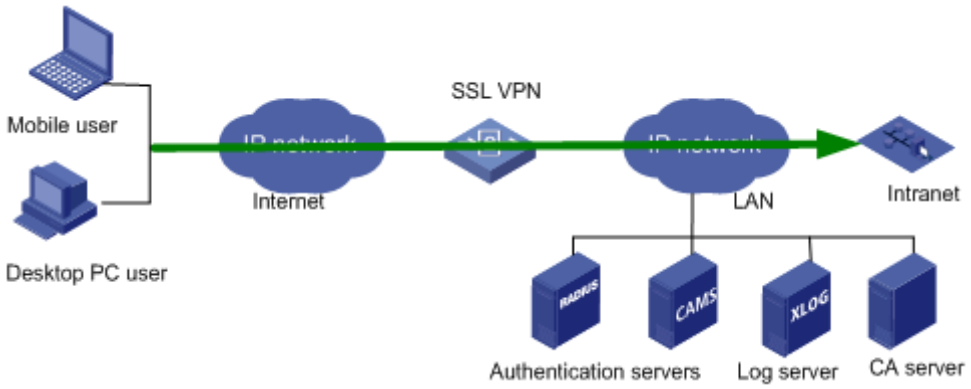


Рисунок 2.6 – VPN

VPN (Virtual Private Network) — це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути декілька, і «зовнішня» мережа, через яку проходять інкапсульовані з'єднання (зазвичай використовується Інтернет).

Підключення до VPN віддаленого користувача робиться за допомогою сервера доступу, який підключений як до внутрішньої, так і до зовнішньої (загальнодоступною) мережі. При підключенні віддаленого користувача (або при установці з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

Прикладом створення віртуальної мережі використовується інкапсуляція протоколу PPP в будь-який інший протокол — IP. Деякі інші протоколи так само надають можливість формування захищених каналів (SSH).

Зазвичай VPN утворюють на рівнях не вище мережевого, так як застосування криптографії на цих рівнях дозволяє використовувати в незмінному вигляді транспортні протоколи (такі як TCP, UDP).

Користувачі Microsoft Windows позначають терміном VPN одну з реалізацій віртуальної мережі — PPTP (Point-to-Point Tunneling Protocol), при чому вона частіше використовується не для створення приватних мереж.

Найчастіше для створення віртуальної мережі використовується інкапсуляція протоколу PPP в який-небудь інший протокол — IP (такий спосіб використовує реалізація PPTP — англ. Point-to-Point Tunneling Protocol) або Ethernet (PPPoE) (хоча і вони мають відмінності). Технологія VPN останнім часом використовується не тільки для створення приватних мереж, але і деякими провайдерами на пострадянському просторі для надання виходу в Інтернет.

При належному рівні реалізації та використанні спеціального програмного забезпечення мережа VPN може забезпечити високий рівень шифрування переданої інформації. При правильному підборі всіх компонентів технологія VPN забезпечує анонімність в Мережі.

VPN з'єднання завжди складається з каналу типу точка-точка, також відомого під назвою тунель. Тунель створюється в незахищеній мережі, якою найчастіше виступає Інтернет. З'єднання точка-точка має на увазі, що воно завжди встановлюється між двома комп'ютерами, які називаються вузлами або peers.

Кожен peer відповідає за шифрування даних до того, як вони потраплять в тунель і розшифровку цих даних після того, як вони покинуть тунель.

Хоча VPN- тунель завжди встановлюється між двома точками, кожен peer може встановлювати додаткові тунелі з іншими вузлами. Для прикладу, коли трьом віддаленим станціям необхідно зв'язатися з одним і тим же офісом, буде створено три окремих VPN- тунеля до цього офісу. Для усіх тунелів peer на стороні офісу може бути одним і тим же. Це можливо завдяки тому, що вузол може шифрувати і розшифровувати дані від імені усієї мережі.

В цьому випадку VPN- вузол називається VPN- шлюзом, а мережа за ним — доменом шифрування(encryption domain). Використання шлюзів зручне з кількох причин. По-перше, усі користувачі повинні пройти через один пристрій, який полегшує завдання управління політикою безпеки і контролю вхідного та вихідного трафіку мережі. По-друге, персональні тунелі до кожної робочої станції, до якої користувачеві потрібно отримати доступ, дуже швидко стануть некерованими (оскільки тунель — це канал типу точка-точка).

За наявності шлюзу, користувач встановлює з'єднання з ним, після чого користувачеві відкривається доступ до мережі(домену шифрування).

SSH (Secure Shell) — мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів). Схожий за функціональністю з протоколом Telnet і rlogin, проте шифрує весь трафік, в тому числі і паролі, що передаються. Схема роботи SSH надана на рисунку 2.7.

Рисунок 2.7 - Робота SSH-тунелю

Криптографічний захист протоколу SSH не фіксований, можливий вибір різних алгоритмів шифрування. Клієнти і сервери, що підтримують цей протокол, доступні для різних платформ. Крім того, протокол дозволяє не тільки використовувати безпечну віддалену оболонку на машині, але і

тунелювати графічний інтерфейс — X Tunnelling (тільки для Unix-подібних ОС або застосунків, що використовують графічний інтерфейс X Window System). Так само SSH здатний передавати через безпечний канал (Port Forwarding) будь-який інший мережевий протокол, забезпечуючи (при належній конфігурації) можливість безпечної пересилки не тільки X-інтерфейсу, але і, наприклад, звуку.

Протокол SSH підтримує декілька варіантів роботи:

1. У першому варіанті тунельований додаток повинен мати налаштування HTTP / SOCKS-proxy для направлення трафіку через локальний proxy-сервер в SSH-тунель. Якщо таких настройок немає, то можна використовувати програми-соксіфікатори, які відправляють трафік через proxy-сервер.
2. У другому випадку можна організувати практично повноцінне VPN-з'єднання і обійтися без настройки SOCKS.

2.6.2 ПОРІВНЯННЯ

Різниця в тому, що технологія proxy забезпечує з'єднання на «прикладному рівні» або іншими словами на рівні додатків, а VPN - це вже мережевий рівень який включає в себе і «прикладний». Ця найголовніша відмінність і не дозволяє обійти VPN-з'єднання, так як всі програми примусово з'єднуються через VPN. Також важливим є примусове шифрування трафіку за допомогою SSL. Якщо зловмисники або системні адміністратори спробують переглянути переданий трафік, то перехопити у них вийде лише сміття, розшифрувати який як правило і тим і іншим не по зубах (розшифровка виробляється на VPN-сервері у якого захистом зберігається ключ сертифіката).

Противники VPN помічають що при шифруванні зростає переданий трафік і як підсумок збільшуються втрати при передачі. Це далеко не так.

VPN-рішення використовують спеціальні бібліотеки які дозволяють стискати передані дані, в результаті втрати не відчутні.

З VPN досить ініціювати з'єднання і запустити необхідний додаток і весь трафік буде передаватися через VPN-канал.

Якщо системний адміністратор прийняв надмірні заходи щодо захисту від proxy- і VPN-з'єднань, досить гнучка настройка VPN-сервера допоможе обійти навіть найсуворіші обмеження.

VPN взагалі потрібен виключно для шифрування трафіку, хоча він і приховує IP його головне завдання приховування трафіку. VPN використовується спільно з proxy.

2.7 ВИСНОВОК

Proxy-сервера, в залежності від виду, реалізують потреби у захисті, забезпечуючи такі функції: анонімність користувача у мережі та організація захищеного каналу зв’язку, попереджуючи фальсифікацію повідомлень.

В залежності від потреб користувача та шляхів використання потрібно вибрати систему з необхідною реалізацією механізму proxy. Для забезпечення максимального захисту створюють ланцюгову ієрархію серверів з використання VPN, SOCKS та Proxy технологій.

3 АНАЛІЗ УРАЗЛИВОСТЕЙ СИСТЕМИ, ЯКА ВИКОРИСТОВУЮ ЗАХИЩЕНІ PROXY

3.1 ХАРАКТЕРИСТИКА СИСТЕМИ TOR

Tor (The Onion Router) - це система проксі-серверів, що дозволяє встановлювати анонімне мережеве з'єднання, захищене від прослуховування. Розглядається як анонімна мережу віртуальних тунелів, що забезпечує передачу даних в зашифрованому вигляді. Написана переважно на мовах програмування Ci, C ++ і Python.

За допомогою Tor користувачі можуть зберігати анонімність в інтернеті при відвідуванні сайтів, веденні блогів, відправці миттєвих і поштових повідомлень, а також при роботі з іншими додатками, що використовують протокол TCP. Анонімність трафіку забезпечується за рахунок використання розподіленої мережі серверів - вузлів. Технологія Tor також забезпечує захист від механізмів аналізу трафіку, які ставлять під загрозу не тільки приватність в інтернеті, але й конфіденційність комерційних таємниць, ділових контактів і таємницю зв'язку в цілому.

Tor оперує мережевими рівнями onion-маршрутизаторів, дозволяючи забезпечувати анонімні вихідні з'єднання і анонімні приховані служби .

3.2 СКАНЕР УРАЗЛИВОСТЕЙ NESSUS

Сканери уразливостей - це програмні або апаратні засоби, що служать для здійснення діагностики та моніторингу мережевих комп'ютерів, що дозволяє сканувати мережі, комп'ютери та програми на предмет виявлення можливих проблем у системі безпеки, оцінювати і усувати уразливості.

Сканери уразливостей дозволяють перевірити різні додатки в системі на предмет наявності «дірок», якими можуть скористатися зловмисники. Також можуть бути використані низькорівневі засоби, такі як сканер портів, для виявлення та аналізу можливих додатків і протоколів, що виконуються в системі.

Роботу сканера уразливостей можна розбити на 4 кроки:

1. Зазвичай, сканер спочатку виявляє активні IP-адреси, відкриті порти, запущену операційну систему та програми.
2. Складається звіт про безпеку (необов'язковий крок).
3. Спроба визначити рівень можливого втручання в операційну систему або програми (може спричинити збій).
4. На заключному етапі сканер може скористатися вразливістю, викликавши збій операційної системи або програми.

Nessus - програма для автоматичного пошуку відомих вад в захисті інформаційних систем. Вона здатна виявити найбільш часто зустрічаються види уразливостей, наприклад:

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

Насамперед використовується для сканування портів і визначає сервіси, що використовують їх. Також проводиться перевірка сервісів по базі уразливостей. Для тестування уразливостей використовуються спеціальні плагіни, написані на мові NASL (Nessus Attack Scripting Language).

База уразливостей оновлюється щотижня, однак для комерційних передплатників є можливість завантажувати нові плагіни без семиденної затримки.

3.3 НАЛАШТУВАННЯ ТА ПЕРЕВЫРКА ЗАХИСТУ СИСТЕМИ

Для початку потрібно налаштувати Proxy з'єднання через Tor. Воно забезпечується використанням локальної машини як SOCKS для забезпечення захищеного доступу в інтернет. Налаштувати Proxy зєднання можна так як показано на рисунку3.1.

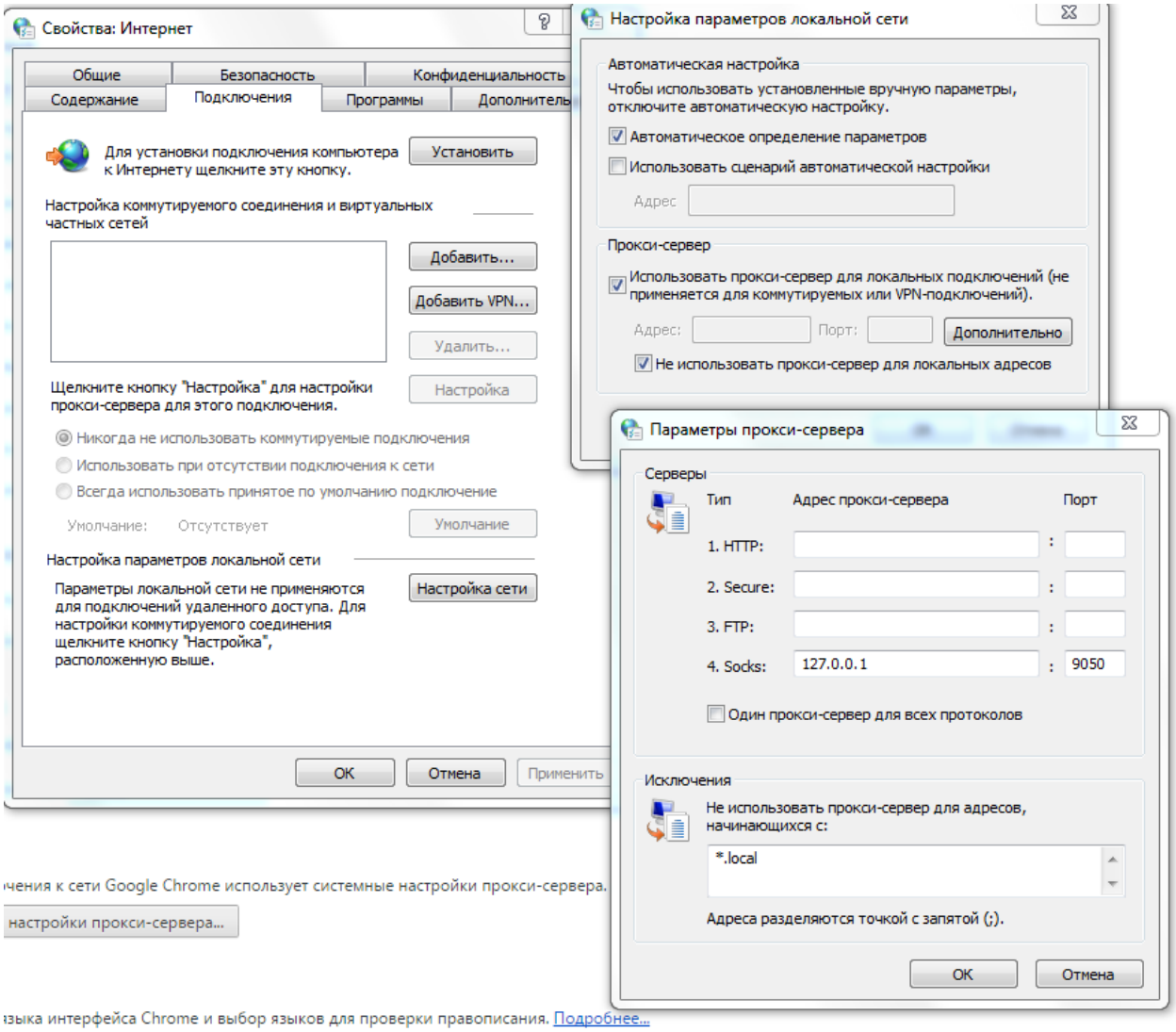


Рисунок 3.1 – Налаштування

Таким чином після встановлення та завантаження система буде забезпечувати вихід комп'ютеру в інтернет через SOCKS з використанням захищених Proxy.

Проаналізуємо наскільки безпечне це з'єдання.

Nessus дозволяє як проводити скани по разу, так і створити шаблон сканування мережі. Для створення скану потрібно заповнити дані , як показано на рисунку 3.2 та вибрати вже готовий з запропонованих шаблон, який будемо модифікувати на рисунку 3.3.

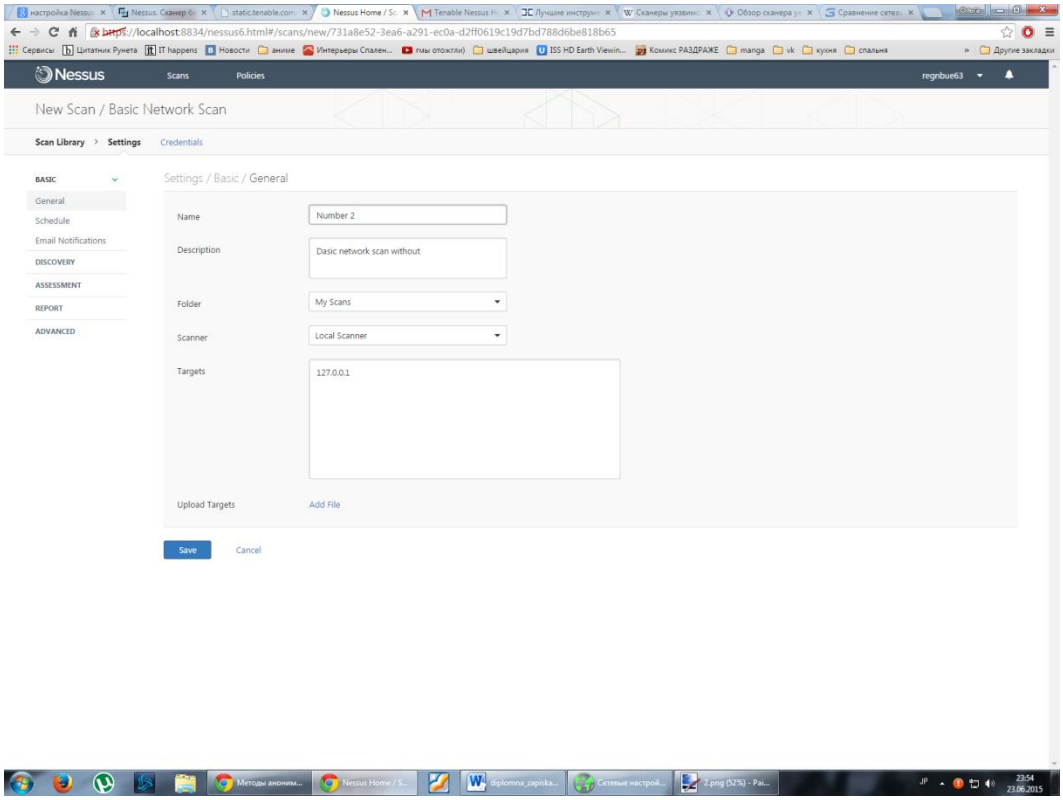


Рисунок 3.2 – Створення скану

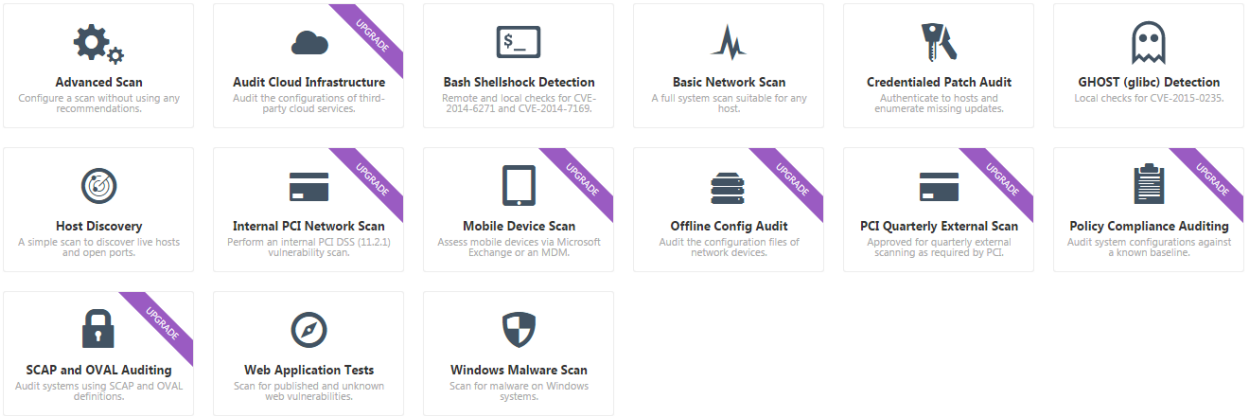


Рисунок 3.3 - Шаблони

Можна створити свій шаблон вибравши потрібні нам параметри. Для цього заповнимо відповідні параметри як показано на рисунках 3.4- 3.6.

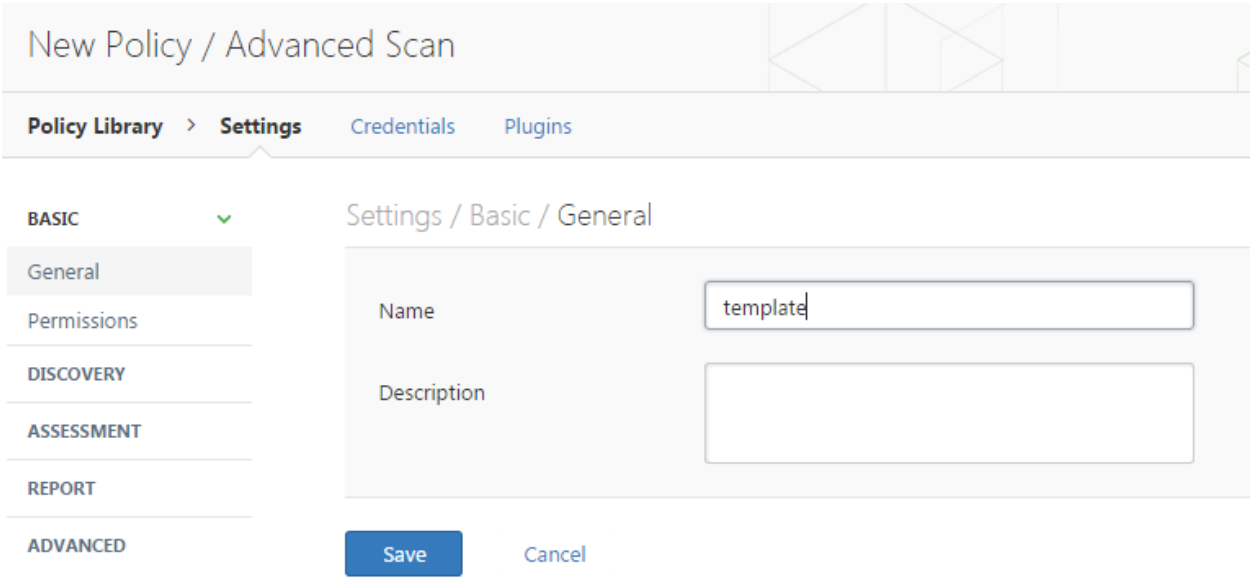


Рисунок 3.4 – Назва

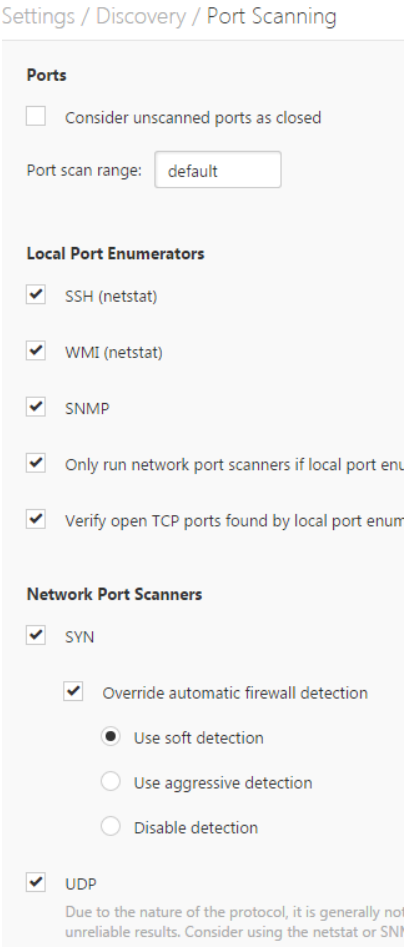


Рисунок 3.5 – Сканування портів

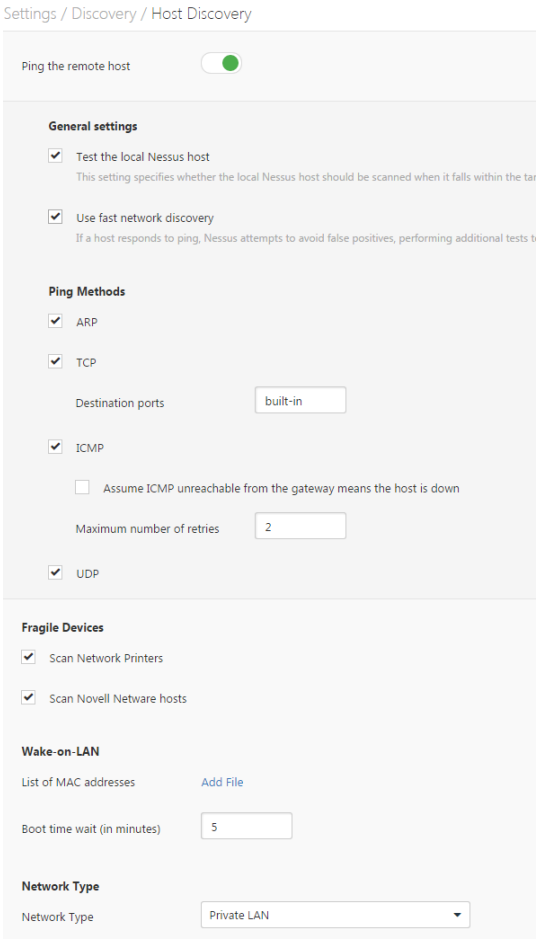


Рисунок 3.6 – Налаштування

Закінчивши ще декілька налаштувань отримаємо шаблон сканеру уразливостей згідно нашим потребам, висунутим до рівня безпеки мережі.

Запустимо його щоб протестувати безпечність з'єднання. Результати можемо побачити на рисунку 3.7.

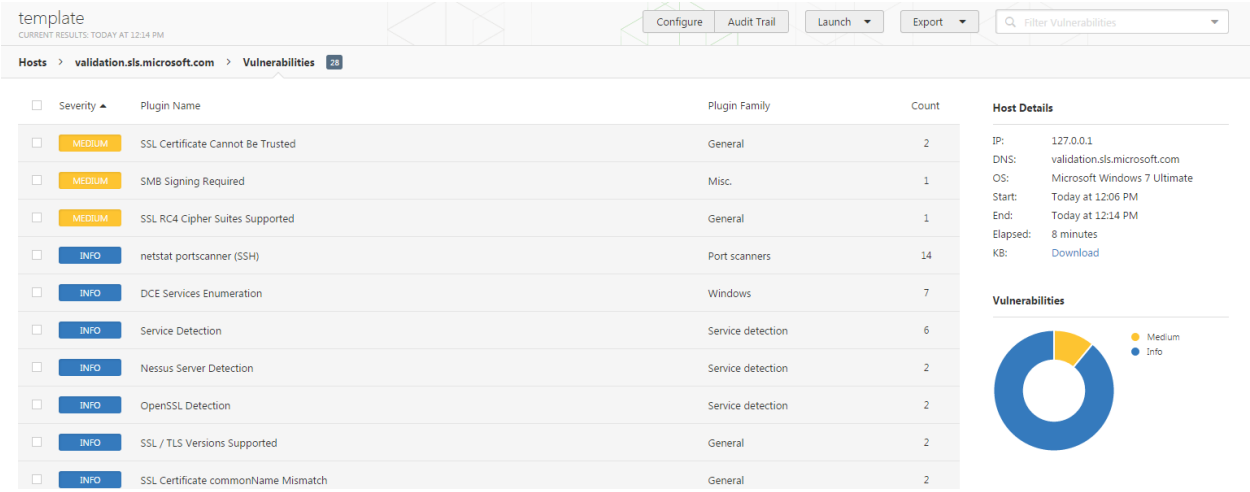


Рисунок 3.7 – Результати сканування

Бачимо середній рівень небезпеки через ненадійність SSL RC4 Cipher, SSL Certificate, SMBSinging. Можна зайти у довідкову інформацію про ці уразливості та прочитати причину їх виникнення та можливість вирішення. Наприклад, про SSL RC4 Cipher бачимо на рисунку 3.8.

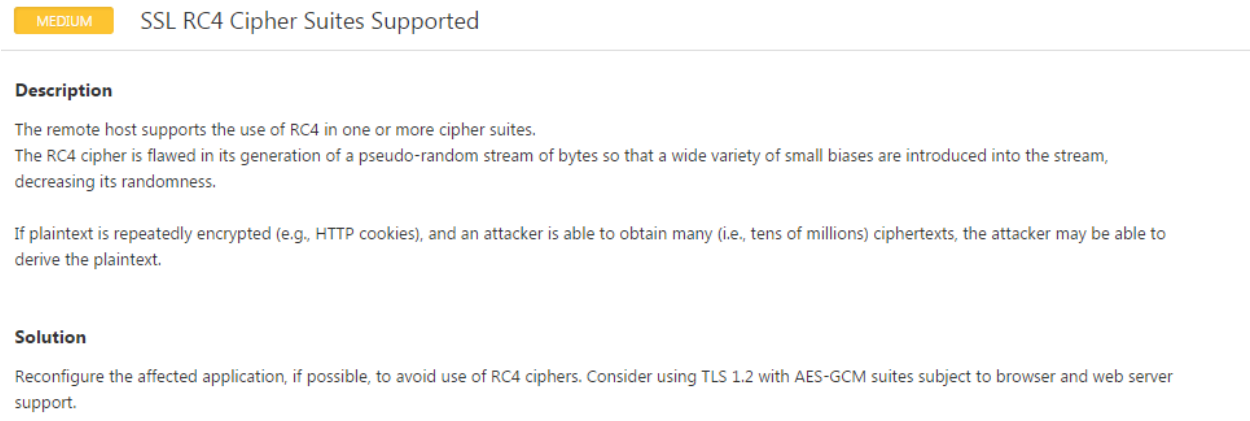


Рисунок 3.8 Уразливість SSL RC4 Cipher

3.4 ВИСНОВОК

Дана система має середній рівень захисту і не підтверджена атакам, немає прослуховування портів. Крім непідтвердженого сертифікати нічого не викликає гострих хвилювань. Ця проблема була вирішена засобами надання хосту Nessus відповідного сертифікату. Використання захищених Proxy-з'єднань задовольняє вимогам, висунутим до рівня захисту системи.

ОХОРОНА ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 ВСТУП

Заходи з охорони праці є важливою складовою для поліпшення умов праці та тим самим підвищення її продуктивності. Це питання з року в рік стає все більш актуальним, оскільки забезпечення здоров‘я людини – це, як обов’язок держави так і підприємств. Впровадження заходів по охороні здоров‘я – важливо для залучення нових кадрів. Для правильної організації процесу трудової діяльності та забезпечення успішного втілення заходів з охорони праці потрібно мати хоча б базові знання в області фізіології праці.

Охорона праці має досить важливий соціальний та економічний аспект, тому так багато уваги їй приділяється як окремими підприємствами так і на державному рівні. На всіх підприємствах, в установах, організаціях повинні створюватися безпечні і нешкідливі умови праці. Забезпечення цих умов покладається на власника або уповноважений ним орган (далі роботодавець). Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизмові, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників. Він не має права вимагати від працівника виконання роботи, поєднаної з явною небезпекою для життя, а також в умовах, що не відповідають законодавству про охорону праці. Працівник має право відмовитися від дорученої роботи, якщо створилася виробнича ситуація, небезпечна для його життя чи здоров'я або людей, які його оточують, і навколишнього середовища. Сприятливі умови праці

благотворно впливають на кар’єрні здібності, розвиток та вдосконалення індивідуальних можливостей та якостей людини, підвищують продуктивність роботи, заохочують її до праці, гарантують зниження аварійності та травматизму.

Даний розділ роботи описує характер приміщення в якому проводились роботи над дипломним проектом.

4.2 АНАЛІЗ УМОВ ПРАЦІ У ПРИМІЩЕННІ

4.2.1 САНІТАРНО-ГІГІЄНІЧНІ ВИМОГИ

Санітарно-гігієнічні вимоги до умов праці повинні бути забезпечені керівниками структурних підрозділів. Серед вимог повинні бути забезпечені такі мінімальні показники згідно з чинними нормативними документами на обладнання одного робочого місця з ПК:

1. Площа – 6,0 м² ;
2. Обсяг – 20,0 м³ (для максимальної кількості працюючих одночасно);
3. Відстань між робочим місцем та стіною з вікном – 1,0 м;
4. відстань між бічними поверхнями комп‘ютерів – 1,2 м;
5. відстань між тильною поверхнею одного комп‘ютера та екраном іншого – 2,5 м;
6. прохід між рядами робочих місць – 1,0 м;

Для заземлених конструкцій у приміщенні (сантехнічні чи водопровідні конструкції) повинен бути забезпечений діелектричний захист від дотику. В кожному такому приміщенні повинна бути передбачена медична аптечка з засобами першої допомоги та система автоматичної пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з розрахунку 2 шт. на кожні 20 кв.м площі приміщення. Підходи до засобів пожежогасіння повинні бути вільними.

4.2.2 ВИМОГИ ДО ОРГАНІЗАЦІЇ РОБОЧОГО МІСЦЯ

Робоче місце обладнане ПК має конструктивно задовольняти ергономічні характеристики оптимальної робочої пози. До них відносяться:

1. Ступні ніг – на підлозі або на підставці для ніг;
2. Стегна - в горизонтальній площині;
3. Передпліччя – вертикально;
4. Лікті - під кутом 70 - 90° до вертикальної площини;
5. Зап'ястя зігнуті під кутом не більше 20° відносно горизонтальної площини;
6. Голова – нахилена на 15 - 20° відносно вертикальної площини;

Для користувачів з основним видом роботи – робота з ПК, периферійні пристрої розміщуються з лівого боку на робочому столі. Повинні бути збережені такі характеристики робочої поверхні столу для ПК, як : висота в межах 680-800 мм та ширина з забезпечення виконання операцій в зоні досяжності моторного поля. Він повинен мати простір для ніг висотою не менше 600 мм, шириною не менше 500 мм, глибиною на рівні колін не менше 450 мм, на рівні витягнутої ноги – не менше 650 мм.

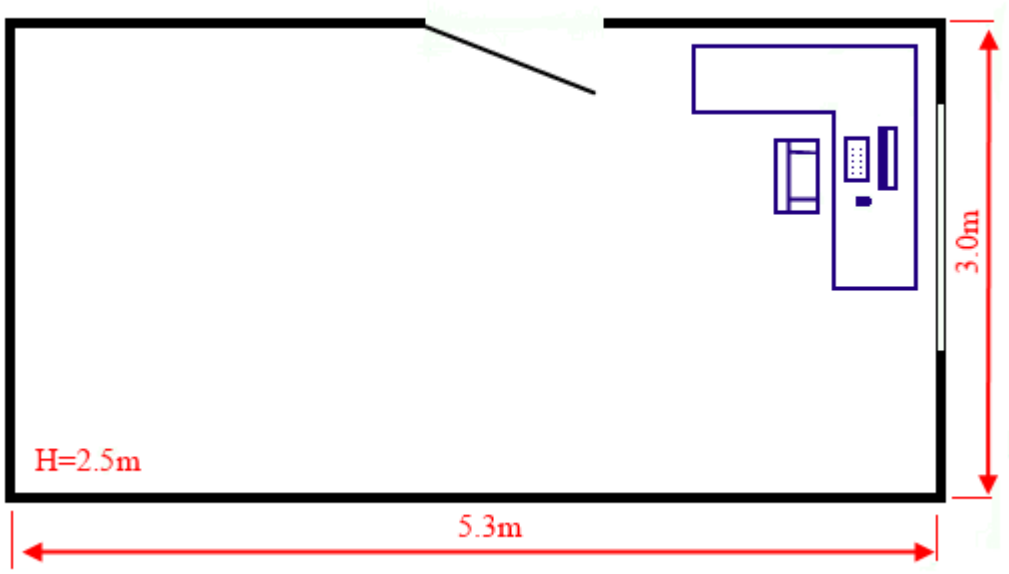
Користувач ПК має мати робоче крісло чи стілець з такими елементами, як : сидіння,спинка, стаціонарні або змінні підлокітники.

Розміщення монітору та клавіатури має відповідати оптимальній відстані від них до очей користувача і з урахуванням розміру алфавітно-цифрових знаків та символів складати не менше ніж 600 мм.

Неправильна організація робочого місця сприяє загальній і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, скривленню хребта й розвитку остеохондрозу.

В даному розділі проводиться аналіз середовища в якому розроблявся програмний продукт на основі санітарних норм України. Приміщення, в

якому розроблявся програмний продукт розташоване на дев‘ятому поверсі 16-поверхового будинку. Його план наведено на мал. 4.1.



Мал. 4.1 – План приміщення

Основні параметри приміщення наведені в таблиці 4.1.

Таблиця 4.1 - Геометричні параметри приміщення

Параметр приміщення	Значення
Довжина, м	5.30
Ширина, м	3.00
Висота, м	2.50
Площа, $м^2$	15.9
Об’єм, $м^3$	39.75

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість монітору, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля: по висоті 900 - 1300 мм, по глибині 400 - 500 мм.

Таблиця 4.2 - Порівняння фактичних і нормативних характеристик робочого місця

Параметр	**Нормативне**	**Фактичне**
Висота робочої поверхні	680-800 мм	750 мм
Глибина робочої поверхні	500-700мм	600 мм
Висота поверхні сидіння	400-500 мм	450 мм
Висота спинки стільця	300+/- 20 мм	320 мм
Регулювання нахилу спинки крісла	1-30°	1-30°
Ширина сидіння	400 мм та більше	480 мм
Глибина сидіння	400 мм та більше	450 мм
Ширина опорної поверхні спинки	380 мм та більше	380 мм
Висота простору для ніг	600 мм та більше	700 мм
Ширина простору для ніг	500 мм та більше	1100 мм
Глибина простору для ніг	650 мм та більше	800 мм
Відстань від екрану до очей	600-700 мм	630 мм

Використовується клавіатура Logitech K310, що повністю відповідає вимогам ергономіки клавіатур, а саме:

1. зміна нахилу поверхні клавіатури повинне лежати в межах від 5° до 15°;
2. висота середнього ряду клавіш - не більш 30 мм;
3. вільний простір від нижнього ряду кнопок до передньої крайки клавіатури повинний мати ширину 80-100 мм тоді, коли крайка піднімається більше чим на 20 мм (для великих рук);
4. вільний простір між крайкою клавіатури і краєм столу повинне мати ширину 80-100 мм у тому випадку, якщо висота передньої крайки клавіатури менше 20 мм (для маленьких рук);
5. розмір контактної площини клавіш, розрахований на антропометричні характеристики вітчизняного користувача, по горизонталі повинний бути не менш 13 мм, по вертикалі - 15 мм;

6. відстань між контактними площинами клавіш не може бути менше 3 мм, що визначається точністю позиціювання пальців;
7. рівний для всіх клавіш робочий хід - 3,0мм;
8. до всіх клавіш повинне прикладатися однакове зусилля натискання 0,25-1,5 Н;
9. клавіатура має можливість переміщуватись щодо монітора в межах 0,5-0,7 м.

Щодо миші, то використовується Genius Traveler 315 Laser, параметри якої також відповідають нормативам:

1. зручний хват забезпечується завдяки глибокій виїмці для великого пальця;
2. кнопки для великого пальця легко доступні, те ж стосується і центральної кнопки.

Ергономіка робочого місця повністю відповідає нормам. Характеристики робочого місця відповідають нормативним вимогам у всьому НПАОП 0.00-1.28-10 та ДСанПіН 3.3.2-007-98).

4.3. РОЗРАХУНКИ ОСВІТЛЕННЯ ТА ЕЛЕКТРИЧНИХ ПРИЛАДІВ ПРИМІЩЕННЯ

4.3.1 ВИМОГИ ДО ОСВІТЛЕННЯ

Робоче місце повинно позиціонуватись відносно вікон так, щоб природне світло було збоку, переважно з лівого. Робоче місце, обладнане ПК повинно бути розташоване так, щоб уникнути попадання в очі прямого світла. Джерела штучного світла рекомендується розташувати з обох сторін від екрану паралельно до напрямку зору. Вікна приміщень повинні мати регулювальні пристрої для відкривання. Якщо джерелом світла в приміщення є штучне освітлення, то застосовуватися, як правило, люмінесцентні лампи.

В приміщені знаходиться одне велике вікно з однієї сторони з такими характеристиками:

Висота: L=1.5 м; ширина: W=2 м, та загальна площа одного вікна: $S=L*W=3$ м^2.

Робота за дисплеєм ПЕОМ за розрядом зорових робіт відноситься до III розряду. При загальному висвітленні освітленість робочого місця повинна становити від 200 до 400 лк.

При штучному освітленні нормуються наступні параметри:

Е (лк) - найменша припустима освітленість;

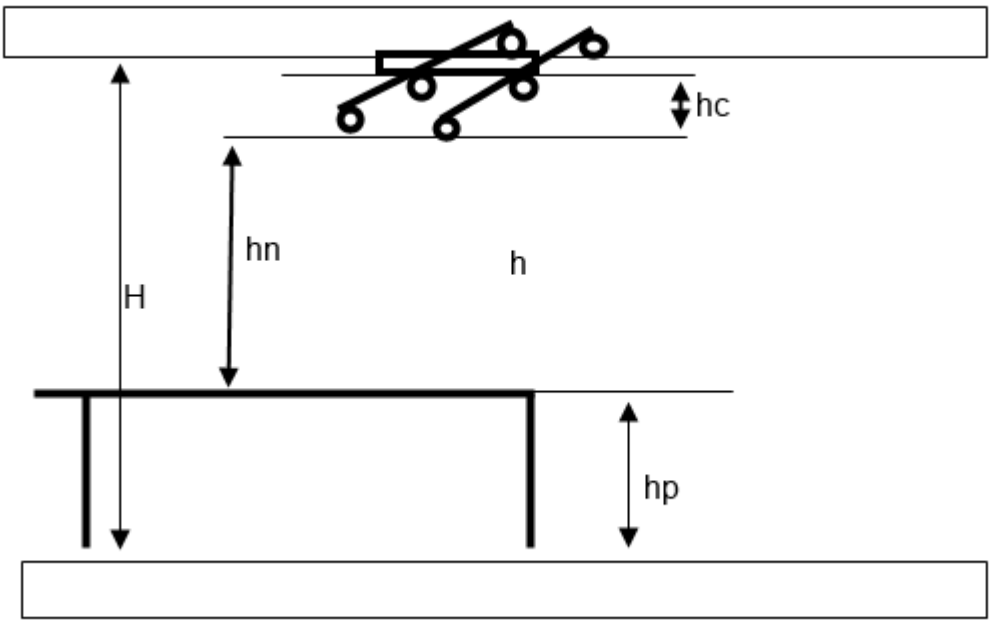
М - показник дискомфорту;

Кп (%) - коефіцієнт пульсації освітленості;

Перевіримо, чи відповідають нормам фактичні параметри штучного освітлення в приміщенні. Номінальний світловий потік лампи білого світіння
ЛБ-40.

$\Phi_л = 3120$ лм.

У приміщенні застосовується світильник, у який встановлено шість ламп.



Мал. 4.2 – Схема освітлення

Висоту підвісу світильника визначимо з формули :

$h = H - h_c - h_p - h_n$,

де

H - висота приміщення, м; h_c - висота світильника, м; h_n - відстань від стелі до підвісу, м; h_p - висота робочої поверхні, м.

Для розглянутого приміщення :

H = 2,5 м; h_c = 0,2 м; h_n = 0,15 м; h_p = 0,75 м.

звідси :

h = 2,5 - 0,2 – 0,15 – 0,75 = 1,4 м.

Лампочки в світильнику розташовані в 2 ряди. Відстань між рядами 0,2 м, відстань від ряду до стіни 1,3 метра. Приміщення має наступні габарити:

довжина А = 5,3 метрів,

ширина В = 3,0 метрів.

Визначимо освітленість у робочій точці. Для розрахунку загальної рівномірної освітленості при горизонтальній робочій поверхні використаємо метод коефіцієнта використання світлового потоку.

Розрахункова формула для світлового потоку світильника має вигляд:

$$Ф_л = \frac{E \cdot K_з \cdot S \cdot Z}{N \cdot n},$$

де

N - число світильників у приміщенні, N = 3*2=6;

n - коефіцієнт використання світлового потоку;

$Ф_л$ - світловий потік ламп;

$K_з$ - коефіцієнт запасу, $K_з$ = 1.5;

Z - коефіцієнт нерівномірності;

S - площа приміщення;

E - освітленість, створювана всіма світильниками.

Звідси одержуємо формулу для розрахунку освітленості на робочому місці :

$$E = \frac{Ф_л \cdot N \cdot n}{K_з \cdot S \cdot Z};$$

Коефіцієнт використання світлового потоку залежить від:

1. ККД, кривій розподілу сили світла світильника;
2. Коефіцієнта відбиття стелі $\boldsymbol{\rho_{сл}}$, стін $\boldsymbol{\rho_{сн}}$ та підлоги $\boldsymbol{\rho_р}$;
3. Висоти підвісу світильників $h_п$;

Індекс приміщення обчислимо за формулою:

$$i = \frac{A * B}{h * (A + B)};$$

де

A та B – параметри кімнати (довжина та ширина відповідно);

h – висота підвісу світильника;

i = (5,3 * 3,0) / (1,5 * (5,3 + 3,0)) = 1,28.

Нам відомо, що стеля свіжопобілена й стіни пофарбовані в світло-фіолетовий кольори, а на підлозі дубова паркетна дошка. Приймаємо:

$\rho_{сл}$ = 70%, $\rho_{сн}$ = 50%, $\rho_{р}$ = 30%;

Звідси Коефіцієнт використання світлового потоку: n = 45%.

Тоді розрахуємо освітленість на робочому місці:

$$E = \frac{3120 \cdot 6 \cdot 0{,}45}{1{,}5 \cdot 15{,}9 \cdot 1{,}1} = 321{,}10 \text{ лк.}$$

Виходячи з того, що по розряду зорової роботи робота за дисплеєм ПЕОМ відноситься до III розряду, тому при загальному освітленні освітленість робочого місця повинна становити від 200 до 400 лк. Фактична освітленість на робочому місці становить 321,10 лк. Виходячи з розрахованих даних маємо задовільні умови існуючих джерел світла для роботи з дисплеєм.

4.3.2 МІКРОКЛІМАТИЧНІ УМОВИ

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря.

Мікрокліматичні умови виробничих приміщень характеризуються такими показниками: температура повітря (°С), відносна вологість повітря (%), швидкість руху повітря (м/с).

Таблиця 4.3 - Значення мікроклімату

Період року	Параметр	Оптимальний	Фактичний
Теплий	Температура	23 – 25 °С	22-25 °С
	Вологість	40 – 60 %	40 %
	Швидкість повітря	≤ 0.1 м/с	
Холодний	Температура	22 – 24 °С	21-23 °С

	Вологість	40 – 60 %	50 %
	Швидкість повітря	≤ 0.1 м/с	

Всі показники мікроклімату у робочому приміщенні задовольняють зазначеним вимогам для робіт Іа категорії (характер роботи - легка) і є задовільними для здоров’я людини. Кондиціонер у приміщенні відсутній. Джерела шкідливих речовин в приміщенні відсутні. Спеціальні заходи з поліпшення або нормалізації цього параметру не потрібні. Радіацією та шкідливим впливом електр-магнітного поля можна знехтувати, адже в сучасних ЕОМ – не виникають. Умови мікроклімату у розглянутому приміщенні задовольняють вимогам встановленим у ДСН 3.3.6.042-99.

4.2.3. ЗАХИСТ ВІД ВИРОБНИЧОГО ШУМУ Й ВІБРАЦІЙ

В досліджуваному приміщенні відсутні джерела вібрації, однак є кілька джерел шуму.

Шум як фізичне явище, являє собою хвильові коливання матеріальних тіл - твердих, газоподібних або рідких. Виникнення звукових відчуттів людини пов'язане з коливаннями повітря.

Зменшення впливу шуму до допустимих величин — одна з незмінних умов оздоровлення умов праці та охорони навколишнього середовища.

Для користувачів, які виконують роботу на обчислювальних машин допустимі рівні звукового тиску та звуку на робочих місцях визначаються, як перша категорія і становлять величини зазначені в таблиці 4.4.

Таблиця 4.4 - Допустимі рівні звукового тиску і рівні звуку для постійного широкосмугового звуку

Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах з середньо геометричними частотами, Гц									Допустимий рівень звуку, дБА
31,5	63	125	250	500	1000	2000	4000	8000	
86	71	61	54	49	45	42	40	38	50

В нашому випадку, приміщення знаходиться далеко від проїжджої частини, метало-пластикові вікна забезпечують звукоізоляцію від зовнішнього середовища. Таким чином список джерел шуму скорочується до:

- Шуму, що створюється системою охолодження ПЕОМ;
- Принтером під час операцій друку.

Сумарний рівень інтенсивності звуку можна розрахувати за формулою:

$$L = 10 \cdot lg\left(\frac{1}{T} \cdot \sum_{i=1}^{n} t_i \cdot 10^{0.1 \cdot L_i} \right)$$

де

T – робочий час протягом дня;

ti – час надходження звуку від і-го джерела;

Li – рівень звукового тиску і-го джерела.

Джерела шуму в кабінеті, що аналізується із зазначенням відповідного рівня звукового тиску приведено в таблиці 4.5.

Таблиця 4.5 – Джерела шуму

Опис джерела	**Рівень звукового тиску**	**Час дії протягом робочого дня**
Кулер ПЕОМ моделі Intel Socket 1155/1156	25 дБА	8 год
ПРИНТЕР HP DESKJET 5150 (друк)	36 дБА	0,5 год

Розрахуємо загальний рівень звукового тиску за формулою:

$$L = 10 \cdot lg\left(\frac{1}{8} \cdot (8 \cdot 10^{0.1 \cdot 25} + 0.5 \cdot 10^{0.1 \cdot 36})\right) = 27.5 \text{ дБА}$$

Отже, фактичний рівень звукового тиску становить 27.5 дБА і не перевищує нормативні 50 дБА навіть під час досить шумної операції друку на принтері. Даний рівень шумів, ультра- та інфразвуків відповідає вимогам ДСН 3.3.6.037-99.

Відстань від екрану монітора повинна складати 600-700 мм. Рівень ЕМ випромінювання повинен відповідати вимогам ДСанПіН 3.3.2.007-98.

Джерелом ЕМ випромінювання в спектрі світлових та рентгенівських хвиль є монітор Dell SP1908FP. Він є сертифікованим на Україні і відповідає умовам НПАОП 0.00-1.28-10.

4.4. ВИМОГИ ДО БЕЗПЕКИ

4.4.1. ЕЛЕКТРОБЕЗПЕКИ

Розглянемо стан електробезпеки у робочому приміщенні:

1. Всі прилади в кабінеті використовують напругу 220 В;
2. Робоче місце з ПК обладнане 6-ма розетками по 220В;
3. Всі нормально струмопровідні елементів (в першу чергу електричні дроти) вкриті ізоляційними матеріалами;
4. Споживачі електроенергії:
    a. Системний блок ПК;
    b. Колонки;
    c. Дисплей;
    d. 1 принтер;
    e. Світильник(6 ламп);
    f. Зарядні пристрої для ноутбуку та телефону;
5. Електромережа в приміщенні розведена в спеціальних каналах стін і підлоги;

З огляду на характер приміщення, можна зробити висновок, що воно відноситься до приміщень без підвищенної електронебезпеки.

ПЕОМ, що використовуються в даному кабінеті підключаються до трифазної мережі і мають захисне занулення (за допомогою окремого захисного нульового провідника). Корпуси ВДТ та принтера виготовлені з пластику і не являються струмопровідними. Щодо корпусів самих ПЕОМ, вони виготовлені зі струмопровідного матеріалу, крім передньої панелі, що виготовлена з пластику.

Дане приміщення задовольняє вимоги до електробезпеки у приміщенні, в якому встановлені ЕОМ , зазначені в НПАОП 0.00-1.28-10.

4.4.2. ПОЖЕЖНА БЕЗПЕКА

Для забезпечення пожежної безпеки в робочому приміщенні були виконані вимоги таких нормативних актів:

1. Кодекс цивільного захисту України;
2. НАПБ Б.01.008-2004 «Правила експлуатації вогнегасників»;
3. НАПБ Б.03.002-2007 Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою;
4. Правила пожежної безпеки в Україні. Наказ Міністерства внутрішніх справ України від 30 грудня 2014 року N 1417;
5. ДБН В.2.5-56:2010 «Системи протипожежного захисту».

Зазначимо потенційні джерела пожежної небезпеки у приміщенні. До них відносяться:

1. Споживачі електроенергії:
    a. Системний блок ПК;
    b. Колонки;
    c. Дисплей;
    d. 1 принтер;
    e. Світильник(6 ламп);
    f. Зарядні пристрої для ноутбуку та телефону;

2. Меблі з горючих і легкозаймистих матеріалів (ДСП, дерево, пластмаса, синтетичні тканини), папір, занавіски на вікнах.

Причина виникнення пожежі в приміщенні може бути незадовільний стан електропристроїв та електропроводки, коротке замикання, перевантаження електромережі, розміщення легкозаймистих матеріалів біля поверхонь, що швидко нагріваються, або не дотримання користувачем правил пожежної безпеки у приміщенні. Робоче приміщення за вибухопожежною і пожежною небезпекою згідно з НАПБ Б.03.002-2007 відноситься до категорії В, тому що у даному приміщенні містяться горючі тверді, волокнисті матеріали. Клас приміщення з пожежонебезпеки — П-IIа, бо в приміщенні є тверді горючі речовини і матеріали.

4.4.3. ДОПОМОГА ПРИ УРАЖЕННІ ЕЛЕКТРИЧНИМ СТРУМОМ

Протікання струму через тіло людини супроводжуєтсья терміч1 ним, електролітичним та біологічним ефектами. Термічна дія струму полягає в нагріванні тканин, випаровуванні вологи тощо, що викликає опіки, обвуглювання тканин та їх розриви парою. Тяжкість термічної дії струму залежить від величини струму, опору проходженню струму та часу проходження. При короткочасній дії струму термічна складова може бути визначальною в характері і тяжкості ураження. Електролітична дія струму проявляється в розкладі органічної речовини (її електролізі), в тому числі і крові, що приводить до зміни їх фізико1хімічних і біохімічних властивостей. Останнє, в свою чергу, призводить до порушення біохімічних процесів в тканинах і органах, які є основою забезпечення життєдіяльності організму. Біологічна дія струму проявляється у подразненні і збуренні живих тканин організму, в тому числі і на клітинному рівні.

Гранично допустимий струм через людину при нормальному (неа1 варійному) режимі роботи електроустановки не повинен перевищува1 ти 0,3 мА для перемінного струму і 1 мА для постійного.

Гранично допустима напруга для людини при нормальному (неава1 рійному) режимі роботи електроустановки не повинна перевищувати 2–3 В для перемінного струму і 8 В для постійного.

При ураженні електричним струмом рятування життя людини залежить від швидкості і правильності дій осіб, що здійснюють допомогу. Передусім потрібно якнайшвидше звільнити потерпілого від дії електричного струму. Якщо неможливо відключити електричне обладнання від мережі, потрібно відразу приступити до звільнення потерпілого від струмопровідних частин, не доторкаючись при цьому до потерпілого.

Заходи долікарської допомоги після звільнення потерпілого залежать від його стану, її потрібно надавати негайно, по можливості на місці події, одночасно викликавши медичну допомогу. Якщо потерпілий не знепритомнів, потрібно забезпечити йому на деякий час спокій, не дозволяючи рухатись до прибуття лікаря. Якщо потерпілий дихає рідко і судорожно, але прослуховується пульс, потрібно негайно зробити йому штучне дихання. При відсутності дихання, розширення зіниць і посиніння шкіри потрібно робити штучне дихання і непрямий масаж серця.

Надавати допомогу необхідно до прибуття лікаря, оскільки є багато випадків, коли штучне дихання і масаж серця повертали потерпілих до життя.

4.5 ВИСНОВКИ

Були розглянуті та проаналізовані дані щодо характеру робочого м’ясця та його ергномічних показників. Обладнання робочого місця відповідають всім, висунутим у законах та нормативно правових актах України, вимогам. Слідуючи приведеним рекомендаціям у облаштуванні робочого місця, можна попередити професійні захворювання, підвищити рівень безпеки праці, попередити виникнення надзвичайних ситуацій та зберегти їх здоров'я.

Повинен бути постійний контороль електро-, газо- і пожежобезпеки у приміщенні. Його можуть забезпечити спеціальні служби охорони праці, а саме відповідні служби і структурні підрозділи підприємства.

Перед початком роботи слід переконатися у справності електропроводки, вимикачів, штепсельних розеток, за допомогою яких обладнання включається в мережу, наявності заземлення комп'ютера, його працездатності.

Щоб уникнути пошкодження ізоляції проводів і виникнення коротких замикань не дозволяється: вішати що-небудь на дроти, зафарбовувати й білити шнури і дроти, закладати дроти і шнури за газові та водопровідні труби, за батареї опалювальної системи, висмикувати штепсельну вилку з розетки за шнур, зусилля повинне бути додане до корпусу вилки. Всі дроти повинні бути ізольовані спеціальними коробами, або закладенні під підлогу для перебачення надзвичайних ситуацій.

Для виключення ураження електричним струмом забороняється: часто вмикати і вимикати комп'ютер без необхідності, торкатися до екрану і до тильної сторони блоків комп'ютера, працювати мокрими руками, працювати на засобах обчислювальної техніки та периферійному обладнанні, що мають порушення цілісності корпусу, порушення ізоляції проводів, несправну індикацію включення живлення, з ознаками електричної напруги на корпусі, класти на обладнання сторонні предмети.

Забороняється під напругою очищати від пилу і забруднення електрообладнання. Забороняється перевіряти працездатність електроустаткування в непристосованих для експлуатації приміщеннях з струмопровідними підлогами, сирих, не дозволяючих заземлити доступні металеві частини. Неприпустимо під напругою проводити ремонт засобів обчислювальної техніки і периферійного обладнання. Ремонт електроапаратури проводиться тільки фахівцями-техніками з дотриманням необхідних технічних вимог.

Після закінчення роботи необхідно знеструмити всі засоби обчислювальної техніки і периферійне устаткування. У разі безперервного виробничого процесу необхідно залишити включеними тільки необхідне обладнання.

ВИСНОВОК

Досліджено механізми захисту розподілених систем та технологія забезпечення proxy з'єднань. Проведений аналіз видів proxy з'єднань, що існують на сьогодні та їх придатність до забезпечення висунутих вимог захист інформації у системі та конфіденційності даних її користувачів.

Проведений аналіз технології формування proxy та їх роль у взаємодії між об’єктами та суб’єктами розподіленої системи. На основі механізму надання доступу у мережі використовуючи proxy сертифікати, проаналізовано можливі варіанти реалізації управляння захистом в розподіленій системі.

Проведений аналіз видів proxy з'єднань, що існують на сьогодні та їх придатність до забезпечення висунутих вимог захист інформації у системі та конфіденційності даних її користувачів.

Використовуюхи засоби та технології, обрані за результатами аналізу, забезпечили відповідний належний захист нашої системи, налаштувавши відповідні захищені proxy з'єднання через систему proxy серверів Tor, й за допомогою сканера уразливостей Nessus виявили її слабкі та сильні сторони. Наведено короткий опис результатів сканування.

Розглянуто альтернативні види забезпечення захищених з’єднані при передачі даних через інтернет та порівняно з технологією proxy з'єднань. За аналізом віддано перевагу proxy з'єднанням через специфіку потреб захисту системи. Висунутий компромісний варіант, що оснований на використанні ланцюгів поєднання відомих технологій забезпечення захищеного захисту доступу до веб-ресурсів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Офіційний сайт Nessus. – Режим доступу : http://www.tenable.com/products/nessus-vulnerability-scanner – Дата доступу: 17.06.2015
2. Офіційний сайт Tor. – Режим доступу : https://www.torproject.org/index.html.en - Дата доступу : 17.06.2015
3. B. Cliford Neuman. Proxy-based authorization and accounting for distributed systems. Technical Report 91-02-01, Department of Computer Science and Engineering, University of Washington, March 1991.
4. Karen R. Sollins. Cascaded authentication. In Proceedings of the 1988 IEEE Symposium on Re-search in Security and Privacy, pages 156-163, April 1988.
5. M. Gasser and E. McDermott. An architecture for practical delegation in a distributed system. In Proceedings of the 1990 IEEE Symposium on Security and Privacy, pages 20-30, May 1990.
6. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. — СПб.: Питер, 2003. — 877 с: ил. — (Серия «Классика computer science»).
7. Защита информации в компьютерных системах и сетях - Владимир Шаньгин - ЛитРес, 2013 – 675с.
8. Санітарні норми мікроклімату виробничих приміщень: ДСН 3.3.6.042-99.
9. ДБН В. 2. 5. – 28– 2006 Збірник 28. «Природне і штучне освітлення».
10. ДСН 3.3.6.039-99. «Державні санітарні норми виробничої загальної та локальної вібрацій» – К.: МОЗ України, 2000.– 45с.
11. ДСН 3.3.6.037-99. «Державні санітарні норми виробничого шуму, ультразвуку та інфразвуку».– К.: МОЗ України, 2000 – 29с.
12. ДСН 3.3.6.042-99 „ Санітарні норми мікроклімату виробничих приміщень” - К.: МОЗ України, 2000.

13. ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин”. №382/3675 , 1998 р.
14. Правила пожежної безпеки в Україні. Наказ Міністерства внутрішніх справ України 30 грудня 2014 року N 1417.
15. НПАОП 0.00-1.28-10 “Правила охорони праці під час експлуатації ЕОМ” – Держгірпромнагляд, № 65 від 26 березня 2010 р.
16. Правила безпечної експлуатації електроустановок, затверджених наказом Державного комітету України по нагляду за охороною праці від 06 жовтня 1997 року № 257, зареєстрованих у Міністерстві юстиції України 13 січня 1998 року за № 11/2451 (НПАОП 40.1-1.01-97).
17. Правила безпечної експлуатації електроустановок споживачів, затверджених наказом Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 09 січня 1998 року № 4, зареєстрованих у Міністерстві юстиції України 10 лютого 1998 року за № 93/2533 (НПАОП 40.1-1.21-98).
18. НАПБ Б.03.002-2007 Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою журнал „Бизнес и безопасность” № 1/2008).
19. НАПБ Б.01.008-2004 «Правила експлуатації вогнегасників».
20. НПАОП 40.1-1.32-01 Правила улаштування електроустановок Мінпаливенерго України, 2010. Вид. 3-тє, перероб. і доп. – 736 с.
21. ДБН В.2.5-56:2010 «Системи протипожежного захисту».