Рисунок 5 – Відображення багатовимірної множини навчальних даних на площину

На рис. 5 видно, що групи листів з теми «реклама промислових товарів» та «реклама побутових послуг» відображаються досить компактно. Це вказує на можливість їх швидкої та якісної класифікації користувачем шляхом візуального аналізу ПК. Зазначимо, на рис. 5 межі кластерів не показані через те, що кластери ПК зайняли несуміжні комірки і їх відображення ускладнює процес візуального аналізу. Однак в автоматичному режимі ПК достовірно розділила листи на три відповідні групи (теми).

IV Висновки

Підвищити ефективність розпізнавання спаму можливо за рахунок використання в антиспамових засобах блоку автоматизованої класифікації листів за допомогою карт Кохонена та ПК.

Перспективним шляхом підвищення рівня захисту електронної пошти є адаптація існуючих методів реферування текстів до використання в системах розпізнавання спаму.

Література: ***1.*** *Цветков В. Я., Булгаков С. В. Спам и некоторые методы борьбы с ним. // http://vio.fio.ru.* ***2.*** *Спам 2004: аналитический отчет – http://www.ashmanov.com.* ***3.*** *Терейковский И. А. Применение семантического анализа содержимого электронных писем в системах распознавания спама / Защита информации – 2006.– № 4, с. 49-60.* ***4.*** *Ежов А. А., Шумский С. А. Нейрокомпьютинг и его применения в экономике и бизнесе / М.: МИФИ, 1998. – 224 с.* ***5.*** *Зиновьев А. Ю. Визуализация многомерных данных / М.: СК Пресс, 2005. - 180 с.* ***6.*** *Заболеева-Зотова А. В. Естественный язык в автоматизированных системах. Семантический анализ текстов: Монография / ВолгГТУ. – Волгоград 2002. – 228 с.*

УДК 004.056.55 (076.5)

РЕАЛІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОМ'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ НА ОСНОВІ ОПЕРАЦІЙНОЇ СИСТЕМИ FREEBSD

Богдан Корнієнко, Леонід Щербак
Національний авіаційний університет

Анотація: **Методологія курсу "Захист інформації в комп`ютерних системах та мережах", що складається із лекцій та лабораторних робіт, має за мету дати студентам фахові знання з основ захисту інформаційної взаємодії у комп`ютерних мережах при їх підключенні до відкритих комунікацій. Лабораторні роботи реалізуються на базі FreeBSD – технологічно зрілої та досконалої операційної системи, що відображено у її стійкості, захищеності та підтримці галузевих стандартів.**

Summary: **The methodology of a rate « Protection of the information in computer systems and networks », that will consist of lectures and laboratory works, has for the purpose to give students a professional knowledge on bases of protection of information interaction in computer networks. Laboratory works are realized on base FreeBSD - technologically and perfect operational system that is displayed in her stability, security and support of branch standards.**

Ключові слова: **Захист інформації, комп`ютерні мережі, операційна система FreeBSD.**

Вступ

Підготовка у вищих навчальних закладах України фахівців за освітнім напрямом «Інформаційна безпека» та розробка методології ряду навчальних дисциплін цього напряму є актуальною задачею, що викликає активну дискусію серед професорсько-викладацького складу та фахівців із захисту інформації. Про це свідчить значна кількість публікацій [1 – 5]. Дана робота присвячена розробці методики викладання курсу "Захист інформації в комп`ютерних системах та мережах" на основі використання операційної системи FreeBSD.

Методологія курсу "Захист інформації в комп`ютерних системах та мережах", що складається з лекцій та лабораторних робіт, має за мету дати студентам фахові знання з основ захисту інформаційної взаємодії у комп`ютерних мережах при їх підключенні до відкритих комунікацій. Курс охоплює основні методи та засоби міжмережного екранування для захисту локальних мереж від несанкціонованого доступу, базові протоколи безпеки та засоби побудови захищених віртуальних мереж. Лабораторні роботи реалізуються на базі FreeBSD – технологічно зрілої та досконалої операційної системи, що відображено у її стійкості,

захищеності та підтримці галузевих стандартів. Сьогодні FreeBSD – повноцінна, багатокористувачева, багатозадачна і багатотермінальна операційна система. FreeBSD функціонує як на персональних комп`ютерах, так і на потужних робочих станціях з RISC-процесорами, під FreeBSD написані потужні САПР і геоінформаційні системи. Своєї масштабованістю FreeBSD через багатоплатформеність на порядок перевершує будь-яку іншу операційну систему.

Постановка задачі

Створення системи захисту – це перша й основна функція адміністратора комп`ютерних мереж. Важливою перевагою операційної системи FreeBSD є наявність інтегрованих механізмів безпеки, що забезпечують захищену роботу комп`ютерної мережі. Системи захисту також реалізуються з урахуванням різних форм атак, що мають своєю метою викликати крах системи або зробити систему недоступною.

Одним з ефективних варіантів реалізації системи захисту може бути багаторівнева система, що створює "рубежі оборони" проти зловмисників. Перший рівень цієї системи утворюють механізми управління доступом до мереж загального використання, а також механізми безпечних комунікацій, що реалізуються у вигляді міжмережних екранів і продуктів захищених віртуальних мереж (VPN). Разом із засобами інтеграції та управління всією ключовою інформацією системи захисту (PKI – інфраструктура відкритих ключів), можна отримати порівняно цілісну, централізовано керовану систему захисту інформації.

Другий рівень включає в себе засоби контролю доступу користувачів до системи, що інтегровані до загальної структури, разом із системою одноразового входу та авторизації.

Третій рівень утворюють засоби антивірусного захисту, засоби аудиту та виявлення атак, а також засоби криптографічного захисту інформації та електронно-цифрового підпису.

Перший рівень	Механізми управління доступом до мереж Міжмережні екрани Захищені віртуальні мережі (VPN) Інфраструктура відкритих ключів (PKI)
Другий рівень	Контроль доступу користувачів до системи Система одноразового входу та авторизації
Третій рівень	Антивірусний захист Аудит та виявлення атак Криптографічний захист інформації Електронно-цифровий підпис

Рисунок 1 – Задачі багаторівневої системи захисту комп`ютерної мережі

Для реалізації основних функціональних компонентів системи захисту комп`ютерної мережі застосовують різні методи та засоби захисту інформації [4, 5]:

захищені комунікаційні протоколи;
засоби криптографії;
механізми авторизації та аутентифікації;
засоби контролю доступу до комп`ютерної мережі;
антивірусні комплекси;
програми виявлення атак та аудиту;
засоби централізованого управління безпечним обміном пакетами даних та повідомленнями відкритими IP-мережами.

В процесі виконання лабораторних робіт студенти отримують необхідні знання в реалізації на базі комп`ютерів із операційною системою FreeBSD сучасних методів захисту інформації в комп`ютерних системах та мережах. Використовуючи лекційний матеріал студенти повинні навчитися створювати сценарії входу до мережі та створювати об'єкти користувачів, реалізовувати авторизований доступ до файлів, змінювати права доступу у користувачів та паролі, розсилати електронну пошту і реалізовувати захист електронної пошти, організовувати мережний друк та взаємодію між користувачами системи, сканувати порти віддаленого комп`ютера, реалізовувати методи захисту інформації за допомогою протоколу IPSec, структуризувати комп`ютерні мережі, відстежувати маршрут проходження пакетів, здійснювати моніторинг і облік мережного трафіку, реалізовувати аутентифікацію користувачів за допомогою захищених протоколів Kerberos IV та Kerberos V, шифрувати файли та паролі, шифрувати хешуванням, читати паролі, генерувати ключі, настроювати, задавати правила та захищати комп`ютерну

мережу за допомогою міжмережного екрану.

Для вивчення основних можливостей ОС FreeBSD студенти створюють сценарії входу до мережі та нові облікові записи користувачів. Сценарій входу користувача визначає оточення для конкретного користувача, в цей сценарій входу заносяться команди, унікальні для кожного користувача. За час процесу входу користувача в систему, FreeBSD виконує декілька дій, які готують користувача та систему до взаємодії одне з одним. Такі дії включають ідентифікацію користувача, ініціалізацію оточення користувача та запуск інтерпретатора команд.

Заходи безпеки для локальної робочої станції можна класифікувати наступним чином:

1. захист `root` та службових облікових записів;
2. захист сервісів, що працюють під `root` та файлів, що виконуються в suid/sgid;
3. захист облікових записів користувачів;
4. захист файлу паролів;
5. захист ядра, пристроїв та файлових систем;
6. швидке виявлення несанкціонованих змін у системі.

Оскільки ОС FreeBSD з самого свого зародження задумувалась як багатокористувачева операційна система, у ній завжди була актуальною проблема авторизації доступу різних користувачів до файлів файлової системи. Схема авторизації доступу, яка застосована в ОС FreeBSD, настільки проста і зручна й одночасно настільки потужна, що стала фактично стандартом сучасних операційних систем.

Важливим аспектом захисту інформації в комп`ютерних мережах є реалізація основних криптографічних алгоритмів для шифрування файлів та паролів. Для передачі паролів використовують шифрування хешуванням. В ОС FreeBSD підтримуються криптографічні алгоритми DES, MD5, Blowfish, а також функція генерації ключів.

У кожного користувача UNIX системи є пароль, пов'язаний з його обліковим записом. Очевидно, що ці паролі повинні бути відомі тільки користувачеві й відповідній операційній системі. Для захисту паролів вони шифруються способом, відомим як ``однобічний хеш'', тобто їх можна легко зашифрувати, але не можна розшифрувати. В операційній системі фіксується тільки пароль у зашифрованій формі. Єдиний спосіб одержати ``звичайний'' пароль це простий перебір всіх можливих паролів. В FreeBSD використовують MD5 як метод шифрування за замовчуванням. MD5 вважається більш безпечним, ніж DES, тому встановлення DES рекомендується в основному з міркувань сумісності. Досить легко визначити, який метод шифрування використовується в FreeBSD. Один зі способів – це перевірка файлу `/etc/master.passwd`. Паролі, зашифровані в хеш MD5 довші, ніж ті, що зашифровано за допомогою DES і починаються із символів 1. Паролі, що починаються із символів $2a$ зашифровані за допомогою Blowfish. Паролі, зашифровані DES, не містять якихось певних ідентифікуючих символів, але вони коротші, ніж паролі MD5 і закодовані в 64-символьному алфавіті, що не містить символу $, тому відносно короткий рядок, що не починається із цього символу – це DES пароль.

Формат паролів, що використовуються для нових паролів, визначається параметром passwd_format в `/etc/login.conf`, що може приймати значення des, md5 або blf.

Kerberos IV та Kerberos V це додаткова мережна система/протокол, що дозволяє користувачам авторизуватися через захищені сервіси на захищеному сервері. Такі сервіси як віддалений вхід, віддалене копіювання, захищене копіювання файлів між системами та інші задачі з високим ризиком стають припустимо безпечними й більш контрольованими.

Kerberos може бути описаний як проксі-система ідентифікації та перевірки, або як захищена зовнішня система аутентифікації. Kerberos надає тільки одну функцію – захищену аутентифікацію користувачів мережі. Він не надає функцій авторизації (що дозволено робити користувачам) або функцій аудита (який користувач, що робить). Після того, як клієнт і сервер скористоались Kerberos для ідентифікації, вони можуть зашифрувати всі з'єднання для гарантування власної безпеки та цілісності даних.

Отже рекомендується використовувати Kerberos з іншими методами безпеки, що надають сервіси авторизації й аудита.

Щоб прозоро для користувача і програми захистити мережні дані ОС FreeBSD використовує протокол IPSec. Цей протокол забезпечує аутентифікацію, конфіденційність, цілісність даних і фільтрацію для TCP/IP трафіку. IPSec реалізований нижче протоколів прикладного рівня і дозволяє захищати сеанс зв'язку будь-якого додатка без його модифікації. Це протокол, що пропонує методи прозорого шифрування й аутентифікації усього інтернет-трафіку на пакетному рівні. Таким чином, навіть потенційно небезпечні протоколи, такі як SMTP, можуть бути надійно захищені. IPSec гарантує, що всі адресатові або вихідні від нього дані не будуть змінені по дорозі. IPSec позбавляє сенсу перехоплення пакетів, тому що їхній вміст неможливе буде розшифрувати, а спроби вставити пакети від імені іншої машини або модифікація трафіку будуть невдалими. За допомогою протоколу IPSec будуємо захищений віртуальний канал.

IPSec заснований на двох ключових компонентах: аутентифікуючому заголовку (Authentication Header - AH) і інкапсулюючому протоколі безпеки (Encapsulating Security Protocol - ESP). AH надає аутентифікацію, підтверджуючи, що присланий відправником пакет дійсно прийшов від нього, і що цей пакет дійсно містить ті дані, що були послані. ESP шифрує дані в пакеті і може так само надавати послуги аутентифікації.

ESP і AH можуть бути використані в режимі транспорту і тунелю. Транспортний режим надає захищене з'єднання між двома точками, тоді як тунель дає VPN-подібне з'єднання (VPN-з'єднання дозволяє користувачам, що знаходяться поза локальною мережею, мати до неї захищений доступ). У транспортному режимі дані пакета підписуються і шифруються. Потім пакет передається за призначенням, де він перевіряється, дешифрується і далі обробляється як звичайний IP пакет. Транспортний режим частіше використовується для передачі даних між двома вузлами. У транспортному режимі походження пакета має значення, тому шифрований трафік не може проходити через мережі, в яких використовується NAT.

У тунельному режимі AH або ESP (або обох) шифрують весь пакет з даними і поміщають результат усередину нового пакета. Цей пакет відправляється на іншу сторону тунелю, де дані розшифровуються і перевіряються. Після цього відновлений первісний пакет обробляється як звичайно, і, якщо необхідно, пересилається до користувача. Тунельний режим найкраще підходить для обміну трафіком між двома маршрутизаторами, або вузлом і маршрутизатором. Через те, вихідний пакет знаходиться в недоторканності, тунельний режим ESP дозволяє пакетам проходити через NAT-мережі. Тунельний режим ESP є відмінним способом захистити незахищені ділянки мережі (наприклад, безпровідні з'єднання).

Робочою групою IP Security Protocol розроблено також і протоколи керування ключовою інформацією: Internet Key Management Protocol (IKMP), протокол керування ключами прикладного рівня, що не залежить від використовуваних протоколів забезпечення безпеки, специфікація Internet Security Association and Key Management Protocol (ISAKMP) і протокол Oakley Key Determination Protocol. Специфікація ISAKMP описує механізми узгодження атрибутів використовуваних протоколів, у той час як протокол Oakley дозволяє встановлювати сесійні ключі на комп'ютери мережі Інтернет.

Облік та моніторинг мережного трафіку здійснюються адміністратором мережі для перевірки і детального аналізу правильності конфігурації мережного програмного забезпечення. Крім того необхідно протидіяти серйозним загрозам перехоплення і розшифровування імен і паролів користувачів, конфіденційної інформації, порушення роботи окремих комп'ютерів і мережі в цілому.

З метою створення комплексної системи захисту необхідно навчитися використовувати міжмережні екрани. Є два типи міжмережних екранів, які використовуються у сучасних комп`ютерних системах. Перший тип називається маршрутизатором з фільтрацією пакетів. Цей тип міжмережного екрана працює на комп`ютері, підключеному до декількох мереж і застосовує до кожного пакета набір правил, що визначає чи передавати цей пакет, чи блокувати. Другий тип, відомий як проксі-сервер, реалізований у вигляді даемонів, що виконують аутентифікацію та пересилання пакетів, можливо на машині з декількома мережними підключеннями, де функція пересилання пакетів у ядрі відключена.

Іноді ці два типи міжмережних екранів використовуються разом, так що тільки певному комп`ютеру (відомому як захищений хост (bastion host)) дозволено відправляти пакети через фільтруючий маршрутизатор у внутрішню мережу. Проксі сервіси працюють на захищеному хості, що звичайно більш безпечно, ніж звичайні механізми аутентифікації.

Маршрутизатор – це машина, що пересилає пакети між двома або декількома мережами. Маршрутизатор з фільтрацією пакетів запрограмований на порівняння кожного пакета зі списком правил перед тим як вирішити, пересилати його чи ні. Більшість сучасних програмних забезпечень маршрутизації має можливості фільтрації, і за замовчуванням пересилаються всі пакети. Для включення фільтрів, необхідно визначити набір правил.

Для визначення того, чи можна пропустити пакет, міжмережний екран шукає в наборі правило, що збігається із вмістом заголовків пакета. Як тільки збіг знайдено, виконується дія, прописана у даному правилі. Дія може полягати у відкиданні пакета, пересиланню пакета, або навіть у відправленні ICMP повідомлення на адресу джерела. Враховується тільки перший збіг, оскільки правила проглядаються в певному порядку. Отже, список правил можна назвати "ланцюжком правил".

Критерій відбору пакетів залежить від використовуваного програмного забезпечення, але звичайно можна визначати правила, що залежать від IP адреси джерела пакета, IP адреси призначення, номера порту джерела пакета, номера порту призначення (для протоколів, що підтримують порти), або навіть від типу пакета (UDP, TCP, ICMP, і т. д.).

Проксі-сервери – це комп'ютери, де звичайні системні даемони (telnetd, ftpd, і т. д.) замінені спеціальними серверами. Ці сервери називаються проксі-серверами, оскільки вони звичайно працюють

тільки із вхідними з'єднаннями. Це дозволяє запускати (наприклад) telnet проксі-сервер на міжмережному екрані і створювати можливість для входу по telnet на міжмережний екран, проходження механізму аутентифікації і одержання доступу до внутрішньої мережі (аналогічно, проксі-сервери можуть бути використані для виходу в зовнішню мережу).

Проксі-сервери звичайно краще захищені, ніж інші сервери, і найчастіше мають більш широкий набір механізмів аутентифікації, включаючи системи "одноразових" паролів, так що навіть якщо хтось довідається, який пароль ви використовували, він не зможе використовувати його для одержання доступу до системи, оскільки термін дії пароля минає негайно після його першого використання. Оскільки пароль не дає доступу безпосередньо до комп'ютера, на якому перебуває проксі-сервер, стає набагато складніше встановити до системи несанкціонований доступ.

Проксі-сервери звичайно мають спосіб додаткового обмеження доступу, так що тільки певні хости можуть одержати доступ до серверів. Більшість також дозволяють адміністраторові вказувати користувачів та комп'ютери, до яких вони можуть звертатися.

В ОС FreeBSD доступний цілий ряд утиліт, що дозволяють реалізовувати міжмережні екрани. Програма ipfw інтегрована в систему, вона дозволяє легко додавати і видаляти правила фільтрації. Це істотно спрощує настроювання робочої конфігурації. Фільтрацію пакетів виконує ядро FreeBSD, оскільки обробка пакетів на такому низькому рівні – це прерогатива ядра. Таким чином, утиліти фільтрації пакетів є усього лише інтерфейсами: вони повідомляють ядру про те, що варто робити з пакетами, які задовольняють визначеним критеріям. Для реалізації міжмережного екрану необхідно розробити політику фільтрації та правильно сконфігурувати ядро FreeBSD.

Програмне забезпечення ipfw, що поставляється з FreeBSD, є системою фільтрації й обліку пакетів, що перебуває в ядрі та має користувальницьку утиліту настроювання. Разом вони дозволяють визначати й переглядати правила, що використовуються ядром при маршрутизації.

Програма ipfw складається із двох зв'язаних частин. Міжмережний екран здійснює фільтрацію пакетів. Частина, що займається обліком IP пакетів, відслідковує використання маршрутизатора на основі правил, подібних тим, що використовуються в частині міжмережного екрана. Це дозволяє адміністраторові визначати, наприклад, обсяг трафіку, отриманого маршрутизатором від певного комп'ютера, або обсяг трафіку WWW, що пересилається. Завдяки тому, як реалізований ipfw, його можна використовувати й на комп'ютерах, що не є маршрутизаторами для фільтрації вхідних і вихідних з'єднань.

Висновки

Основні принципи побудови системи захисту інформації та методи захисту інформації, що викладаються у лекційному курсі, можуть бути реалізовані практично при виконанні лабораторних робіт на базі ОС FreeBSD. Наведені методи захисту інформації можуть використовуватись при розробці комп`ютерних систем керування технологічними процесами з використанням мікропроцесорних контролерів, включених у мережі обміну інформацією.

Література: ***1.*** *Бабак В. П., Корченко О. Г. Інформаційна безпека та сучасні мережеві технології. Англо-українсько-російський словник термінів. Київ: НАУ, 2003. - 670 с.* ***2****. Богуш В. М., Юдін О. К. Інформаційна безпека держави Навчальний посібник для студентів напряму 1601 "Інформаційна безпека" // видавництво К.: „МК-Прес" 2005 р. -432 с.* ***3.*** *Головань С. М., Дудикевич В. Б., Зачепило В. С., Пархуць Л Т., Хорошко В. О., Щербак Л. М. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом // Підручник для студентів базового напряму 1601 "Інформаційна безпека". Вид. "Львівська політехніка". – м. Львів, 2005. 311 с.* ***4.*** *Корнієнко Б. Я., Фомін М. М., Щербак Л. М. Захист інформації в комп`ютерних системах та мережах (модульні технології навчання). Навчально-методичне видання, Київ: НАУ. – 2004, 107 с.* ***5.*** *Корнієнко Б. Я., Щербак Л. М. Захист інформації в комп`ютерних системах та мережах, частина 2 (модульні технології навчання). Навчально-методичне видання, Київ: НАУ. – 2005, 139 с.* ***6.*** *Корнієнко Б. Я., Щербак Л. М. Захист інформації в комп`ютерних системах та мережах, (модульні технології навчання). Навчально-методичне видання, Київ: НАУ. – 2006, 64 с.*