12. Які правила експлуатації ЕОМ існують в даній інформаційній системі та чи були порушені ці правила (робота на ЕОМ в неробочий час, самовільне підключення модему до ЕОМ та інсталяція програмного забезпечення тощо) ?
13. Чи знаходиться порушення правил експлуатації в причинному зв'язку із знищенням, копіюванням, модифікацією інформації?
14. Визначити електронні адреси, на які зроблена несанкціонована передача конкретної інформації (визначити отримувача інформації) та визначити що було передано;
15. Визначити всі випадки набору на клавіатурі критичної інформації і словосполучень тощо.

Таким чином, впровадження технології спостереженості комп'ютерних систем з застосуванням СБ "СОВА" надає ефективний засіб щодо боротьби і розслідуванню "кіберзлочинів".

Література: 1. Collin Barry C. The Future of Cyber Terrorism // Proceedings of 11th Annual International Symposium on Criminal Justice Issues. The University of Illinois at Chicago, 1996. 2.International Computer Crime Squads. The report of the President's Commission on Critical Infrastructure Protection, 1997. http://www.pccip.gov/report_index.html. 3.Голубєв В.О. Комп'ютерні злочини в банківській діяльності. — Запоріжжя, 1997. С.16-18. 4.Mark M. Pollitt. CYBERTERRORISM - Fact or Fancy? FBI Laboratory. 5. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. // Департамент спеціальних телекомунікаційних систем та технічного захисту інформації Служби безпеки України. – Київ, 1999. 6. Кримінально-процесуальний кодекс України: науково-практичний коментар. — Київ, 1995. — 639 с.

УДК 681.513
РОЗПІЗНАВАННЯ СЕРВІСІВ TCP/IP ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

Олексій Новіков, Сергій Кащенко
Фізико-технічний інститут Національного технічного університету України "КПІ".

Анотація: **В доповіді розглядаються питання підвищення рівня безпеки комп'ютерних мереж шляхом використання детекторів вторгнень. В якості методу виявлення порушень безпеки запропоновано розпізнавання аномальної поведінки сервісів TCP/IP за допомогою нейронної мережі зворотного поширення.**
Summary: **In the article questions of computer networks security enhancement by instrusion detection systems usage. Recognition of TCP/IP services anomalous behavior using backpropagation neural network is proposed as method of security violations detection.**
Ключові слова: **нейронні мережі, Інтернет, безпека комп'ютерних систем, детектори вторгнень.**

I Вступ

Існує три групи засобів, що їх використовують системи захисту інформації від несанкціонованого доступу: аутентифікація, контроль доступу та аудит. Засоби аутентифікації встановлюють істинність однієї сутності обчислювальної системи для іншої. Засоби контролю доступу визначають, що одна сутність системи може робити з іншою (тобто з ресурсами та об'єктами, що вона їх репрезентує), і потребують як передумову використання засобів аутентифікації. Засоби аудиту збирають дані про активність системи та аналізують їх з метою виявити ознаки порушень безпеки. При цьому аналіз може відбуватись як у "відкладеному" режимі, так і в режимі реального часу. Інструменти аналізу мають назву "детектори вторгнень".

Внаслідок бурхливого зростання глобальної комп'ютерної мережі Інтернет, а також зростаючої популярності Інтернет-технологій при побудові корпоративних комп'ютерних мереж, одним з найбільш поширених способів мережевої взаємодії стає використання стеку протоколів TCP/IP. При цьому сутностями, що діють в мережі як розподіленій обчислювальній системі, є процеси, що їх виконують комп'ютери-абоненти [1]. Кожен процес на певному комп'ютері має унікальну адресу, або порт, що за її допомогою взаємодіє з іншими процесами. В загальному випадку процес може володіти кількома портами, а також динамічно займати і звільняти порти в процесі роботи. Пара адреса комп'ютера-номер порта унікальним чином ідентифікує процес у мережі в цілому, і носить назву "сокет". Також необхідно зазначити, що існує традиційно встановлена відповідність між номером

порта та видом процесу, що його займає. Так, порт 80 звичайно використовується процесом WWW-сервера, порт 21 – FTP-сервера і т.д. Серверний процес носить назву "сервіс".

Власне протокол TCP оперує на сеансовому рівні еталонної моделі взаємодії відкритих систем (OSI). Одиницею мережевого обміну на даному рівні є з'єднання, або віртуальний канал, що встановлюється, виконує розподілений у часі двосторонній обмін даними з забезпеченням їх цілісності та руйнується. В кожен момент часу унікальним ідентифікатором з'єднання є пара сокетів [1].

Задача аутентифікації в такому розподіленому середовищі здебільшого реалізується за допомогою засобів асиметричної криптографії. В якості механізмів контролю доступу використовуються міжмережеві екрани (брандмауери, firewalls), що дозволяють обмежити доступ з однієї мережі в іншу певними адресами та номерами портів шляхом фільтрації пакетів та з'єднань.

Щодо останньої задачі, аудиту, то вона донедавна в мережевих середовищах не вирішувалась взагалі, або ж вирішувалася на рівні підсистеми аудиту комп'ютера-абонента мережі. Такий підхід має наступні недоліки:

- вразливість журналів аудиту операційних систем (вони можуть бути спотворені або знищені зловмисником у випадку, якщо комп'ютер буде вдало атаковано);
- відчутна втрата обчислювальних ресурсів на створення журналів аудиту (до 20% часу CPU);
- різноманіття використовуваних операційних систем (і, відповідно, форматів журналу аудиту);
- наявність часового інтервалу між власне подією та її реєстрацією;
- існування атак, що не відбиваються на журналах аудиту.

Це призвело до створення нового класу детекторів вторгнень - мережевих моніторів безпеки. В якості вхідних даних такий монітор отримує дані обміну просто з мережі. Це досягається завдяки шинній топології Ethernet-мереж, де кожен абонент принципово здатен отримати всі дані, що передаються даним сегментом мережі [2]. В більш складних випадках, якщо треба спостерігати декілька сегментів водночас та в комутованих мережах, використовуються дані мережевого обміну, отримані за допомогою span-портів ("перекриваючих" портів) маршрутизаторів та комутаторів, або ж за допомогою спеціального апаратного забезпечення.

II Методи аналізу даних аудиту

Методи аналізу, що їх використовують детектори вторгнень, можна поділити на дві групи: виявлення аномалій та виявлення зловживань.

В основі методів виявлення зловживань лежить ідея про те, що можна репрезентувати відомі атаки у вигляді шаблонів або сценаріїв з тим, щоб здійснювати пошук таких шаблонів у журналах аудиту або даних мережевого обміну. При цьому одним з найважливіших питань є створення таких шаблонів, що дозволяють виявляти всі варіанти тієї чи іншої атаки. До цієї групи методів відносять використання експертних систем, виявлення зловживань за допомогою моделей (model-based), аналіз переходів стану та метод зіставлення шаблонів (pattern matching)[3].

При використанні **експертних або продукційних систем** як механізму аналізу даних аудиту на них покладають наступні задачі:

1) символьний вивод факту атаки або зловживання з наявних даних;
2) комбінація різноманітних показників роботи спостережуваної обчислювальної системи з метою побудови загальної картини стану безпеки.

Основним недоліком експертних систем є їх нездатність обробляти неявно задані послідовності подій.

При **виявленні зловживань за допомогою моделей** створюються описи ознак порушень безпеки (моделі), і відбувається пошук цих ознак у вхідних даних. Детектор вторгнень в цьому випадку складається з трьох модулів: модулю прогнозу (anticipator), модулю планування (planner), та інтерпретатору. Модуль прогнозу використовує активні моделі порушень, щоб передбачити, який з кроків сценарію має бути наступним. Модуль планування далі перетворює ці кроки у формат вхідних даних детектора вторгнень. І, нарешті, інтерпретатор здійснює пошук цих даних серед вхідних даних.

При використанні методу **аналізу переходів стану** система, що спостерігається, репрезентується у вигляді графу-діаграми переходів стану. По мірі аналізу даних здійснюються переходи з одного стану в інший. Щоб відбувся якийсь з переходів треба, щоб задовольнялась відповідна умова. Підмножина станів є "скомпрометованими", і якщо система приходить в них, то детектор вторгнень сигналізує про порушення безпеки.

В основі **методу зіставлення шаблонів** лежить опис відомих атак у вигляді кольорових мереж Петрі. При цьому в якості кольорових фішок виступають добуті з вхідних даних детектора події, а на переходи додатково накладаються специфічні умови.

Незважаючи на всі переваги методів виявлення зловживань (високу точність та обчислювальну ефективність) всі вони мають один фундаментальний недолік – за їх допомогою можна виявити лише відомі різновиди порушень безпеки.

Основою **методів виявлення аномалій** є припущення, що всі порушення безпеки обчислювальної системи обов'язково є аномаліями в їх роботі. Це значить, що можна створити "профіль" нормальної роботи системи і розглядати всі статистично значущі відхилення від нього як спроби порушити безпеку [3]. Оскільки насправді множини порушень безпеки та аномальних станів системи не співпадають, а лише перетинаються, іноді виникають дві наступні ситуації:

а) фальш-позитиви (false-positives) – ситуації, що не є порушеннями безпеки, але є аномальними станами і, таким чином, розглядаються як порушення;

б) фальш-негативи (false-negatives) – ситуації, що є порушеннями безпеки, але не є аномальними станами і, таким чином, не розглядаються як порушення.

Основною проблемою цієї групи методів є знаходження таких "порогів" відхилень, що мінімізують фальш-позитиви і фальш-негативи.

До цієї групи методів належать статистичний метод, метод прогнозуючого породження шаблону та нейромережевий метод.

Статистичний метод виявлення аномалій полягає в виборі певної групи характеристик роботи спостережуваної системи і обчислення діапазонів цих характеристик при нормальній роботі системи. Ця група показників, що власне носить назву "профіль", може оновлюватись з часом, тим самим адаптуючись до змін характеристик роботи. Серйозним недоліком даного методу є ігнорування зв'язку між показниками.

При використанні методу **прогнозуючого породження шаблону** намагаються передбачити наступні події, спираючись на ті події, що вже відбулися. Так, наприклад, може існувати правило:

$$E1 - E2 \rightarrow (\ E3=80\%,\ E4=15\%,\ E5=5\%\ ).$$

Це значить, що якщо виникає подія E1, а за нею E2, то існує імовірність 0.8, що наступною подією буде E3, імовірність 0.15 – E4 та імовірність 0.05 – E5. Переглядаючи свою базу правил, детектор вторгнень може визначити поточну послідовність подій як високоімовірну, або як малоімовірну, і в останньому випадку сигналізувати про порушення безпеки.

Нейромережевий метод виявлення аномалій полягає у використанні для аналізу вхідних даних штучних нейронних мереж. Останні являють сильнозв'язані набори простих обчислювальних елементів, що трансформують вхідні набори даних у бажані вихідні. Результат перетворення визначається характеристиками елементів та вагою зв'язків між ними. Змінюючи вагу зв'язків можна "навчити" нейронні мережу будь-якому виду перетворень [4].

Штучні нейронні мережі мають ряд переваг над статистичними методами аналізу:

- по-перше, статистичні методи не можуть адекватно описувати складну взаємодію між вхідними параметрами;
- по-друге, статистичні методи залежать від припущень щодо природи вхідних даних (наприклад, Гаусове розподілення, квазістаціонарні процеси і т.п.). Ці припущення можуть бути невірними, що призведе до високого рівня фальш-негативів та фальш-позитивів. Нейронні мережі не потребують таких припущень;
- по-третє, часто буває важко виділити, які з характеристик роботи обчислювальної системи є значущими для детектора вторгнень, а які – ні. Нейронна мережа в процесі навчання автоматично встановлює слабкі зв'язки з незначущими вхідними параметрами;
- по-четверте, набагато простіше і швидше перенавчити нейронну мережу для нових умов, ніж створити заново програмне забезпечення, що реалізує статистичні алгоритми;
- по-п'яте, завдяки "вбудованій" можливості кластеризації, нейромережеві методи досить просто піддаються масштабуванню.

Метод виявлення аномалій за допомогою штучних нейронних мереж вже продемонстрував свою високу спроможність розрізняти користувачів за їх поведінкою у детекторах вторгнень, орієнтованих на журнали аудиту [5,6]. Щодо мережевих моніторів безпеки, то в цій галузі не було проведено великої кількості досліджень [7,8], причому дослідження були сфокусовані перш за все на моніторингу мережі в цілому. Таким чином, актуальним стає створення монітору безпеки, що використовував би нейронні мережі для спостередження за суб'єктами мережевої взаємодії.

III Експерименти

В даній роботі поставили собі за мету відповісти на запитання: чи можна за допомогою нейронної мережі розрізнити один від іншого серверні процеси (сервіси) TCP/IP мереж на основі характеристик TCP-з'єднань? Власне, питання полягає у тому, чи демонструють сервіси достатню відтворюваність характеристик своїх TCP-з'єднань для своєї однозначної ідентифікації? Якщо відповідь на це запитання буде позитивною, то можна побудувати детектор вторгнень, що вказуватиме на можливі порушення безпеки кожен раз при виявленні TCP-

з’єднання з певним сервісом, характеристики якого (з’єднання) не відповідають встановленим для цього сервісу. Нас не цікавила поведінка клієнтських процесів в силу нефіксованості їх місцезнаходження (тобто номерів портів). Також ми не прагнули навчити нейронну мережу розпізнавати атаки, використовуючи в числі вхідних даних адресу та номер порту процесу, як це зроблено в [7], оскільки такий підхід не є цілком коректним.

Як характеристики TCP-з’єднання ми використовували:

- загальну кількість байт, переданих з’єднанням в обох напрямках;
- середню, максимальну та мінімальну кількість байт, передаваних одним пакетом в обох напрямках (оскільки в кожному з’єднанні присутні службові пакети з нульовою довжиною, мінімальна кількість байт в пакеті бралася мінімальна ненульова);
- дисперсію кількості байт для послідовності пакетів з’єднання, також в обох напрямках;
- кількість пакетів, що несуть службові флаги протоколу TCP: URG, PUSH та RST, також в обох напрямках;
- індикатори нормального відкриття та нормального закриття з’єднання;
- тривалість з’єднання в мілісекундах;
- кількість з’єднань на сокеті даного сервісу на момент відкриття даного з’єднання.

Таким чином, усього 20 характеристик.

Як інструмент збору даних використовувалась програма WinDimp – Windows-версія відомої програми для ОС UNIX TCPDump. Ця програма переводить мережеву карту комп’ютера в так званий promiscous-режим, і таким чином, мережева карта починає отримувати не тільки адресовані їй Ethernet-пакети, але всі пакети, що передаються даним сегментом мережі. Прослуховуючи сегмент, WinDump виконує розбір та фільтрацію пакетів відповідно з заданими опціями та друкує відфільтровані пакети у відповідному протоколу форматі. Ми використовували WinDump з опцією “tcp” для відбору тільки TCP-пакетів та перенаправляли друк програми в файл. Приклад формату отриманих даних можна побачити на рисунку 1.

Подібні WinDump інструменти збору даних носять назву “сніфери”.

Далі отримані дані проходили обробку за допомогою створеної нами програми-конвертеру, що розбирала отриманий від WinDump файл на сесії та обчислювала характеристики кожної сесії, тим самим створюючи вхідний файл для симулятора нейронної мережі.

Як симулятор нейронної мережі використовувалась програма Pittnet. Ця програма дозволяє:

- вибирати тип нейронної мережі, що буде використовуватись. В даний час підтримуються 4 типи мереж: зворотнього поширення, адаптивного резонансу, відображення Кохонена та RBF-мережі;
- задавати конфігурацію нейронної мережі;
- тренувати, або ж навчати мережу;
- тестувати навчену нейромережу;
- зберігати результати тренування, результати тестування та власне мережу в файлах та загружати ці файли в разі необхідності.

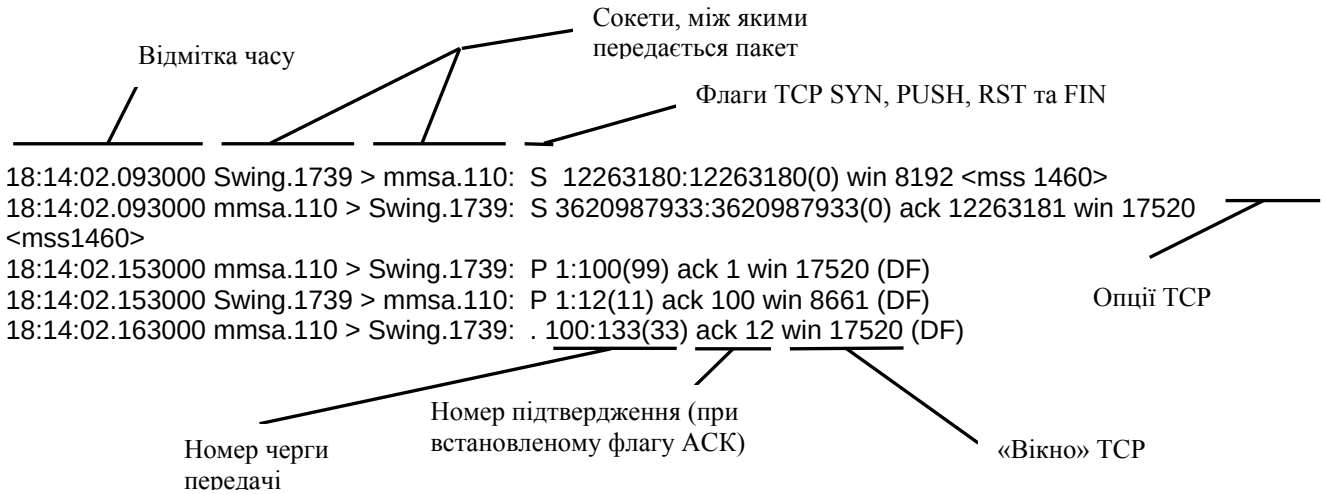

Рисунок 1

Нами використовувались три нейронні мережі зворотнього поширення наступних конфігурацій:

20 x 5 нейронів
20 x 10 x 5 нейронів
20 x 10 x 10 x 5 нейронів

Тобто 20 вхідних, 5 вихідних нейронів та по 10 нейронів в одному або двох прихованих шарах двох останніх мереж.

Як функція активації для всіх нейронів використовувалась сигмоїдна функція:

$$f(x) = \frac{1}{1+e^{-x}} \qquad (1)$$

Нормалізація даних характеристик з'єднань здійснювалась вбудованою в Pittnet процедурою нормалізації наступним чином:

$$Нормалізоване \quad значення = \frac{Поточне \quad значення - Мінімальне \quad значення}{Максимальне \quad значення - Мінімальне \quad значення} \qquad (2)$$

Результати експерименту зазначені на рисунку 2.

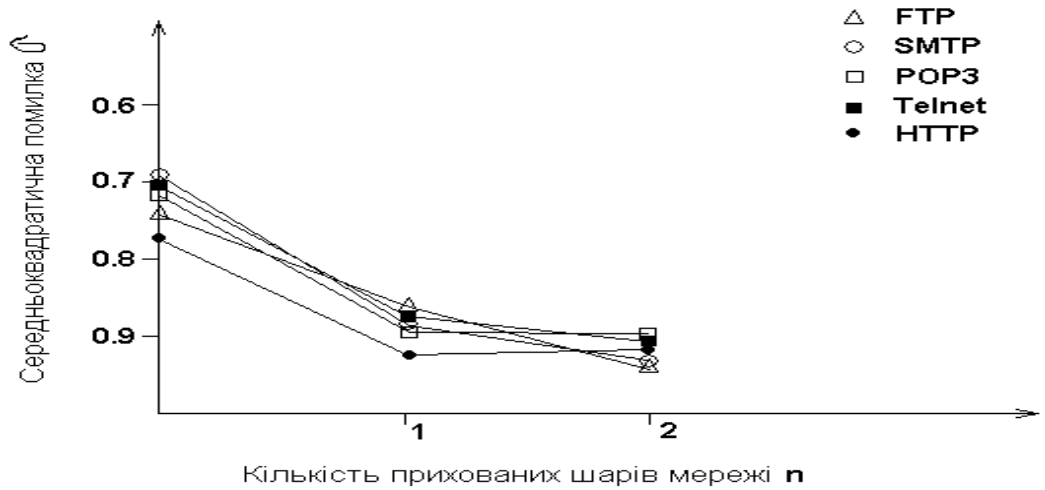

Рисунок 2

IV Висновки

Розглянуто питання підвищення рівня захищеності комп'ютерних мереж, побудованих за Інтернет-технологією, шляхом використання спеціалізованих мережевих засобів аудиту – детекторів вторгнень типу моніторів безпеки. Протягом експерименту нейронну мережу зворотнього поширення було навчено розпізнавати сервіси TCP/IP, базуючись на даних – характеристиках їх з'єднань. Якщо навчена таким чином нейромережа не зможе правильним чином розпізнати те чи інше з'єднання TCP як таке, що належить до того чи іншого сервісу, це сигналізуватиме про значні зміни поведінки даного сервісу, що, в свою чергу, може бути ознакою атаки на нього. Загалом продемонстровано перспективність використання нейронних мереж як засобу аналізу даних мережевого аудиту.

Література: 1. Postel J. E. Transmission Control Protocol. RFC 793.– 1981.– September. ***2****. Mukherjee B., Heberline L.T., Levitt K.N. Network Intrusion Detection//IEEE Network.– 1994.– May/June.–P.26.* ***3****. Lunt T.F. A Survey of Intrusion Detection Techniques//Computers& Security.–1993.– June.– P.405-418.* ***4****. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика. - М.: Мир. - 1992. - 240 с.* ***5****. Ryan, J., Lin, M., Miikkulainen, R. Intrusion Detection with Neural Networks//AI Approaches to Fraud Detection and Risk Management: Papers from the 1997 AAAI Workshop (Providence, Rhode Island). – 1997. – P.72-79.* ***6****. Tan K. The Application of Neural Networks to UNIX Computer Security// Proceedings of the IEEE International Conference on Neural Networks. – 1995. –Vol.1.– P. 476-481.* ***7****. Кеннеди Дж. Нейросетевые технологии в диагностике аномальной сетевой активности. Перевод А.В. Лукацкого, Ю.Ю. Цаплева и В.П. Сахарова –* ***www.infosec.ru.*** ***8****. Cansian A., Moreira E., Carvalho A., Bonifacio Jr.J. Network Intrusion Detection Using Neural Networks //Proceedings of the International Conference on Computational Intelligence and Multimedia Application, Gold Coast,Australia.–1997.– February.– P.276 - 280.*