УДК 347.731:681.3

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ СПОСТЕРЕЖЕНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИНАМИ

Володимир Голубєв
Запорізький юридичний інститут МВС України

Анотація: **У статті розглядається застосування системи безпеки "СОВА" на основі використання технології спостереженості комп'ютерних систем для розслідування кіберзлочинів.**
Summary: **The article regards the application of a security system "Network Remote Monitor" based on computer systems accountability technology for cybercrimes investigation.**
Ключові слова: **автоматизована система, кіберзлочини, технологія спостереженості.**

Впровадження сучасних інформаційних технологій привело до виникнення нових видів злочинів, при здійсненні яких використовуються обчислювальні системи, новітні засоби телекомунікації і зв'язку, засоби негласного отримання інформації тощо. Збільшується кількість так званних кіберзлочинів з використанням сучасних інформаційних технологій, розкрадання готівки і безготівкових грошових коштів. Термін "кіберзлочин" (cybercrime) молодий і утворений сполученням двох слів: кіберпростір і злочин. Термін кіберпростір (у вітчизняній літературі частіше зустрічаються терміни "віртуальний простір", «віртуальний світ») позначає (відповідно до визначення з книги "Новий словник хакера" Еріка С. Реймонда) інформаційний простір, що моделюється за допомогою комп'ютера, у якому існують визначеного роду об'єкти або символьне уявлення інформації - місце, де діють комп'ютерні програми і переміщуються дані [1].

Так за даними американського Інституту Комп'ютерної Безпеки (Computer Security Insitute) на підставі дослідження, проведеного за завданням Міжнародної Групи з Комп'ютерних Злочинів (International Computer Crime Squads) ФБР США [2], був складений звіт щодо комп'ютерної безпеки і проблеми кіберзлочинів, а також наведені найбільш поширені методи атак і порушень:

- метод грубої сили (**brute-force**) - 13,9%. Підбір паролів, ключів і іншої ідентифікаційної або аутентифікаційної інформації;
- підміна IP-адресу (**IP-spoofing**) - 12,4%. Метод атаки, при якому зловмисник змінює IP-адреси пакетів, переданих по Internet таким чином, щоб вони виглядали "внутрішніми" для мережі, де кожний вузол довіряє адресній інформації іншого;
- ініціювання відмови в обслуговуванні (**denial of service**) - 16,3%. Вплив на мережу або окремі її частини з метою порушення порядку штатного функціонування;
- аналіз трафіка (**sniffer**) - 11,2%. Перегляд і розшифровування переданих даних із метою збору паролів, ключів і іншої ідентифікаційної або аутентифікаційної інформації;
- сканування (**scanner**) - 15,9%. Метод атаки з використанням програм, що послідовно перебирають можливі точки входу в систему (наприклад, номера TCP-портів або телефонні номера) із метою встановлення шляхів і можливостей проникнення;
- підміна, нав'язування, знищення, переупорядкування даних або заміна вмісту повідомлень, переданих по мережі (**data diddling**) - 15,6%.

Відповідно до статистичних даних, отриманих ФБР США у результаті аналізу спроб проникнення в 220 комп'ютерних систем американської мережі "MILNET" [4], уразливими виявилися 20% паролів, які використовувалися. У 98% випадків адміністратори атакованих систем для з'ясовування обставин підозрілої активності навіть не намагалися зв'язатися з організацією, мережа якої після вторгнення зловмисника використовувалася ним для нападу на інші мережі. 8% систем надали зловмиснику інформацію про свій поточний статус і працюючих користувачів по введеним їм найпростішим запитам типу sysstat, who тощо. 1% систем надали обмежений доступ до баз даних і систем електронної пошти. У 2% випадків зловмисник спромігся проникнути в систему під ім'ям легального користувача. 2% систем надали зловмиснику привілею адміністратора автоматизованої системи.

Як бачимо є дуже багато шляхів навмисного несанкціонованого доступу до даних і втручання в процеси обробки і обміну інформацією в автоматизованих системах. Під *автоматизованою системою (АС)* ми розуміємо – організаційно-технічну систему, що реалізує інформаційну технологію і об'єднує операційну систему, фізичне середовище, персонал і інформацію, яка обробляється [5]. Надійно побудована система захисту інформації - важлива складова безпеки роботи АС, а в випадку скоєння кіберзлочину надає можливість правоохоронним органам у проведенні розслідування.

Як суб'єктами застосування засобів і заходів у кримінальному судочинстві виступають його учасники, оскільки вони беруть участь у процесі доказування і здійснюють збирання, дослідження, оцінку і використання

криміналістичної інформації. Однак, внаслідок різного рівня їх процесуального становища, форми і межі використання ними спеціальних засобів і знань відрізняються. Для дізнавача і слідчого такі засоби є знаряддям у праці і правоохоронній діяльності, вони мають право використовувати їх безпосередньо (ст. 114 КПК України) або опосередковано, застосовуючи для цього спеціальні знання спеціаліста (ст. 75 КПК України) [6]. Аналогічні правові норми є у законодавстві багатьох країн світу. Таким чином законність застосування технології спостереженості при розслідуванні кіберзлочинів характеризується правовою стороною допустимості і свідчить про відповідність використання цих технологій для збирання криміналістичної інформації.

Для вирішення зазначених проблем, одним з підприємств України (http://www.anna.zp.ua), була розроблена система безпеки "СОВА", яка проходить сертифікацію у Департаменті спеціальних телекомунікаційних систем та технічного захисту інформації Служби безпеки України. Додатково на кафедрі оперативно-розшукової діяльності Запорізького юридичного інституту МВС України, у рамках Американсько-Українського науково-дослідницького партнерства, проводяться дослідження з метою розробки рекомендацій щодо розкриття та розслідування транснаціональних комп`ютерних злочинів (кіберзлочинів) з використанням мережі Internet.

Система безпеки “СОВА” (далі по тексту СБ "СОВА") - це мережева програмно-апаратна система безпеки, яка призначена для автоматизованого забезпечення спостереженості комп'ютерних (обчислювальних) систем користувачів автоматизованої системи, які працюють під керуванням операційної системи Windows 95/98/NT виробництва фірми Microsoft (США) в автоматизованих системах, що базуються на TCP/IP мережах.

В СБ "СОВА" реалізована така функція захисту як ***спостереженість*** (accountability) — властивість *комп'ютерної (обчислювальної) системи*, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення *політики безпеки інформації* і/або забезпечення відповідальності за певні дії. Система безпеки здійснює такі дії як ***реєстрація*** (audit, auditing), що забезпечує збирання та аналіз інформації щодо використання користувачами і процесами функцій та об’єктів, які контролюються комплексом засобів захисту та веде ***журнал реєстрації*** (audit trail) у вигляді упорядкованої сукупності реєстраційних записів, кожен з яких заноситься комплексом засобів захисту за фактом здійснення контрольованої події.

Використання технології спостереженості комп'ютерних систем з застосуванням СБ "СОВА", має суттєве значення у розслідуванні кіберзлочинів, пов`язаних з **“людським чинником”**, що дає можливість правоохоронним органам вирішувати наступні задачі:

1. з'ясування окремих фактів витоку інформації з локальної мережі;
2. відновлення знищених або модифікованих зловмисником файлів, встановлення точного часу і дати цих дій;
3. встановлення факту несанкціонованої інсталяції программного та аппаратного забеспечення;
4. розшифрування закодованих зловмисником файлів;
5. реєстрація спроб неавторизованого доступу;
6. встановлення авторства, місця та часу підготовки конкретних файлів;
7. встановлення рівня професійної підготовки окремих осіб в області інформаційних технологій;

Проведення розслідування починається з аналізу журналу реєстрації СБ "СОВА", у якому орган дізнання зможе отримати відповіді на наступні питання:

1. Який склад програмних засобів встановлено на ЕОМ та чи можна за допомогою цих засобів здійснити дії, що інкримінуються обвинуваченому?
2. З якими інформаційними ресурсами працював користувач ЕОМ?
3. Чи не є виявлені файли копіями інформації, що знаходилася на конкретній ЕОМ?
4. Чи не є виявлені документи, документами, які створювалися на конкретній ЕОМ, якщо вони були потім знищені на ЕОМ?
5. Коли (день, місяць, час, хвилина), ким (кому належить той чи інший пароль доступу), на якій ЕОМ (кому належить робоче місце) проводилася робота на ЕОМ з конкретною інформацією?
6. Чи не є виток інформації результатом інсталяції спеціалізованого програмного забезпечення?
7. Чи не є представлені файли з програмами заражені вірусом, і якщо так, то яким саме, яка його дія (знищення, копіювання, модифікація, передача інформації в мережу інформації чи таке інше)?
8. Чи не є представлені файли з програмами файлами з включеним до їх складу програмних закладок, і якщо так, то яким саме, яка його дія (знищення, копіювання, модифікація, передача інформації в мережу інформації чи таке інше)?
9. Чи не є представлені тексти на паперовому носії записами початкового коду програми, і яке призначення цієї програми?
10. Чи не є представлені тексти на паперовому носії записами, які потім набиралася конкретним користувачем ЕОМ в конкретному електронному документі?
11. Чи зазнавала дана комп'ютерна інформація знищення, копіювання, модифікації?

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