УДК 004.056.5

КОМП'ЮТЕРНА БЕЗПЕКА – ЦІЛІСНІСТЬ ДАНИХ І КОНФІДЕНЦІЙНІСТЬ ІНФОРМАЦІЇ

Костікова М. В. [1], Гетало Д. І. [2], Гура В. О. [3]
[1] канд. техн. наук, доцент, [2, 3] студенти групи ДМ-21-20
ХНАДУ, м. Харків, Україна
E-mail: [1] kmv_topaz@ukr.net, [2] getalo30@gmail.com, [3] torriaaa007@gmail.com

Кожного дня хакери піддають загрозі багато ресурсів, стараючись здобути до них доступ. Цьому сприяють два основні фактори. По-перше, це повсюдне проникнення Інтернет. Зараз до мережі Інтернет приєднані мільйони пристроїв. Багато пристроїв будуть приєднані до неї в майбутньому.

Отже ймовірність доступу хакерів до уразливих пристроїв безперервно зростає. Крім того, широке розповсюдження Інтернет позволяє хакерам обмінюватися інформацією в глобальному масштабі. По-друге, це спільне поширення простих у застосовуванні операційних систем і оточень розроблення. Цей чинник різко знижує рівень знань і досвід, які необхідні хакеру.

Мережеві атаки настільки ж різні, як і системи, проти яких вони спрямовані. Деякі атаки різняться складністю. Інші може здійснити простий користувач, навіть не здогадуватися, які наслідки може мати його діяльність. Для оцінки різновидів атак необхідно знати окремі обмеження, спочатку властиві протоколу TCP / IP. В умовах ранніх версій Інтернет-протоколу (IP) були неприсутні вимоги безпеки. Саме тому багато реалізації IP є передусім уразливими. Згодом стали запроваджувати засоби безпеки для IP.

Однак з огляду на те, що спершу способи захисту для протоколу IP не розроблялися, всі його реалізації стали доповнюватися всілякими мережевими процедурами, послугами та продуктами, що знижують загрози, властиві цим протоколом. Далі розглянемо типи атак, які застосовуються проти мереж IP, і перерахуємо способи боротьби з ними.

1. Сніфери пакетів (перехоплення та аналізу мережевого трафіку сторонніми особами).

Основними методами захисту від сніфінгу є:

- аутентифікація;
- комутована інфраструктура;
- антисніфери;
- криптографія.

Автентифікація. Міцні засоби автентифікації є першим способом захисту від сніфінга пакетів. Під «міцним» ми розуміємо такий метод автентифікації, який тяжко уникнути. Зразком такої автентифікації є одноразові паролі. Якщо хакер узнає цей пароль за допомогою сніфер, ця інформація буде даремна, тому що в цей момент пароль вже буде використаний і виведено з ужитку.

Комутована інфраструктура. Якщо, для прикладу, у всій організації використовується комутований Ethernet, хакери можуть отримати доступ тільки до трафіка, що приходить на той порт, до якого вони підключені.

Антисніфери. Полягає в установці апаратних чи програмних засобів, які розпізнають сніфери, які працюють у вашій мережі. Вони включаються в загальну систему захисту. Антисніфери замірюють час реагування хостів і визначають, чи не доводиться хостам обробляти «зайвий» трафік.

Криптографія. Дієвий засіб боротьби зі сніфінгом пакетів не запобігає перехоплення і не розпізнає роботу сніфера, але робить цю роботу марною. Якщо канал зв’язку є криптографічно захищеним, це значить, що хакер підхоплює не повідомлення, а зашифрований текст.

2. IP-спуфінг.

IP-спуфінг виникає, коли хакер, що перебуває усередині корпорації або поза її, видає себе за санкціонованого користувача. Це можна зробити двома способами. По-перше, хакер може застосувати IP-адресу, або вповноважити зовнішню адресу, якій дозволяється доступ до певних ресурсів мережі. Атаки IP-спуфінга часто є первинною точкою для інших атак. Зазвичай обходиться вставкою неправильної інформації або шкідливих команд у звичайний потік

даних. Для двобічного зв'язку хакер повинен переробити всі таблиці маршрутизації, щоб направити трафік на хибну IP-адресу. Якщо головне завдання полягає в отриманні від системи вагомого файлу, відповіді додатків не мають значення. Якщо ж хакеру удається змінити таблиці маршрутизації і направити трафік на неправильну IP-адресу, хакер отримає всі пакети і зможе відповідати на них так, ніби він є санкціонованим користувачем.

Загрозу спуфінга можна ослабити (але не усунути) за допомогою таких заходів:

Контроль доступу. Щоб знизити ефективність IP-спуфінгу, відрегулюйте контроль доступу на відсікання будь-якого трафіка, що надходить з зовнішньої мережі з вихідною адресою, який повинен влаштовуватися усередині вашої мережі. Якщо санкціонованими є і деякі адреси зовнішньої мережі, даний метод стає недійовим.

Фільтрація RFC 2827. Ви можете припинити спроби спуфінга незнайомих мереж користувачами вашої мережі. Для цього варто відбраковувати будь-який вихідний трафік, початкова адреса якого не є однією з IP-адрес вашої організації. У наслідку відбраковується весь трафік, який не має вихідної адреси, очікуючого на певному інтерфейсі.

3. Відмова в обслуговуванні (Denial of Service – DoS).

DoS – найбільш відома форма хакерських атак. Проти атак подібного типу найважче створити стовідсотковий захист. Атаки DoS різняться від атак інших типів. Атака DoS робить вашу мережу недоступною для простого використання викликано перевантаження мережі, функціонування мережі, програми або операційної системи.

Існує три способи зниження загроз DoS атак.

Функції анти-спуфінга. Ці функції, як мінімум, зобов'язані включати фільтрацію RFC 2827. Якщо хакер не зможе затаїти свою справжню особистість, він навряд чи відважиться провести атаку.

Функції анти-DoS. Ці функції нерідко лімітують кількість напіввідкритих каналів у будь-який момент часу.

Обмеження обсягу трафіка. Організація може попрохати провайдера (ISP) обмежити обсяг трафіка.

4. Парольні атаки.

Хакери вміють проводити парольні атаки за допомогою великого ряду методів, таких як простий перебір, «троянський кінь», IP-спуфінга і сніфінг пакетів. Одноразові паролі або криптографічна аутентифікація практично зводять такий тип загроз.

5. Атаки типу Man-in-the-Middle.

При атаки типу Man-in-the-Middle хакер отримує доступ до пакетів, що передаються по мережі. Атаки проводяться з метою крадежу інформації, перехоплення поточної сесії і одержання доступу до часних ресурсів мережи. З атаками типу Man-in-the-Middle можна ефективно боротися тільки за допомогою шифрування.

6. Атаки на рівні додатків.

Атаки на рівні додатків можна провести різними засобами. Найпоширеніший з них полягає у вживанні добре визначних слабкостей серверного програмного забезпечення (sendmail, HTTP, FTP). Вживаючи ці слабкості, зловмисники отримують доступ до комп'ютера від імені користувача, що зареєстровано в додатки.

Найбільша проблема з атаками на рівні додатків полягає в тому, що вони часто використовують порти, які мають доступ для проходу через міжмережевий екран. Наприклад, хакер, який експлуатує відому слабкість Web-сервера, найчастіше використовує для атаки TCP порт 80. Оскільки Web-сервер дозволяє користувачам Web-сторінки, міжмережевий екран зобов'язаний надавати доступ до цього порту.

Повністю виключити атаки на рівні додатків неможливо. Головне тут – хороше системне адміністрування.

7. Мережева розвідка.

Мережева розвідка – це збір інформації про мережу за допомогою доступних даних і додатків. Для мережевою розвідки використовується запити DNS, сканування портів і exo-тестування. DNS запити дозволяють отримати інформацію, про власника того чи іншого домену і які адреси цього домену привласнені. Exo-тестування адрес, розкритих за допомогою DNS, дозволяє дізнатися,

які хости дійсно роблять у даному середовищі. Діставши список хостів, хакер вживає засоби сканування портів, для складання повного списку послуг, які надаються цими хостами. У результаті зловмисник отримує інформацію, яку може використати для взлому.

8. Зловживання довірою.

Власне кажучи, цей тип дій не є «атакою» або «штурмом». Він являє собою зловмисне вживання відносин довіри, що існують у мережі. Класичним зразком такого зловживання є ситуація в периферійній частині корпоративної мережі.

Ризик зловживання довірою можна знизити за рахунок більш грубого контролю ступенів довіри в межах своєї мережі. Відносини довіри повинні обмежуватися певними протоколами і, по можливості, аутентифікуватися не тільки по IP-адресам, а й за іншими параметрами.

9. Переадресація портів.

Переадресація портів є різновидом зловживання довірою, коли зіпсований хост використовується для передачі через міжмережевий екран трафіка, який в іншому випадку був би неодмінно відбракований. Зовнішній хост має можливість підключитися до хосту загального доступу (DMZ), але не до хоста, встановленого з внутрішньої сторони міжмережевого екрану. Хост загального доступу може підключатися і до внутрішнього, і до зовнішнього хосту. Якщо хакер загарбає хост загального доступу, він зможе встановити на ньому програмний засіб, що перенаправляють трафік з зовнішнього хоста прямо на внутрішній хост. Завадити хакеру приладнати на хості свої програмні засоби може хост-система IDS (HIDS).

10. Несанкціонований доступ.

Несанкціонований доступ не може прийматися окремим типом атаки. Більшість мережевих атак проводяться задля отримання несанкціонованого доступу. Щоб підібрати логін Telnet, хакер повинен спочатку отримати підказку Telnet на своїй системі. Після підключення до порту на екрані появлятиметься повідомлення. Якщо після цього хакер продовжить спроби доступу, вони будуть прийматися несанкціонованими.

Засоби боротьби з несанкціонованим доступом доволі прості. Головним тут є скорочення або повна знищення можливостей хакера з отримання доступу до системи за допомогою несанкціонованого протоколу.

11. Віруси і додатки типу «Троянський кінь».

Робочі станції фінальних користувачів дуже вразливі для вірусів і «Троянських коней». «Троянський кінь» – це не програмна вставка, а повноцінна програма, яка виглядає як благодійна програма, а на ділі здійснює шкідливу роль. Зразком типового «Троянського коня» є програма, яка виглядає, як звичайна гра, поки користувач грає у гру, програма поширює свою копію електронною поштою кожному абоненту адресної книги цього користувача. Кожен абонент одержує поштою гру, та може викликати її подальше поширення.

Для боротьби з вірусами та «Троянськими кіньми» використовується ефективні антивірусні програми забезпечення, які працюють на рівні користувача та на рівні мережі

Політика безпеки – це формальний набір правил, яким зобов’язані підкорятися працівники, які мають доступ до корпоративної технології та інформації.

Засоби мережі в себе включають:

- Хост мережі (персональні комп’ютери; включає операційні системи, програми, дані хостів).
- Пристрої мережі (маршрутизатори, міжмережеві екрани).
- Дані мережі (дані, які передаються з даної мережі).

Опорними елементами політики у галузі безпеки є ідентифікація, цілісність і активна перевірка. Ідентифікація запобігає загрозі знеособлення і несанкціонованого доступу до ресурсів і даних. Цілісність забезпечує захист від підслуховування і маніпулювання даними, підтримуючи конфіденційність і незмінність переданої інформації.

Активна перевірка (аудит) значитиме перевірку правильності виконання елементів політики безпеки.

Цілісність – це елемент, який включає захист пристрою інфраструктури мережі (логічний і фізичний доступ), безпеку периметра і конфіденційність даних. Безпека фізичного доступу може виражатися

в розстановці обладнання мережі в навмисне створених для цього оснащення шафах, які мають обмежений доступ.

Приватність даних може забезпечуватися протоколами безпеки на транспортному рівні SSL і Secure Shell Protocol (SSH), які виконують безпечну передачу даних між клієнтом і сервером.

Засіб SOCKS є рамковою будовою, що дозволяє додаткам клієнт / сервер в доменах TCP і UDP сприятливо і безпечно вживати послуги мережевого міжмережевого екрану.

Останнім визначним елементом системи безпеки є аудит, який портібний для стеження і верифікації процесу дослідження політики безпеки. Для випробування ефективності інфраструктури системи безпеки, аудит безпеки має відбуватися часто, через рівні інтервали часу. Він також зобов'язаний включати перевірки установки новітньої системи, методи для визначення можливих шкідницьких дій будь-кого з внутрішнього колективу і можливої присутності своєрідного класу проблем (нападу типу «відмова в сервісі»), а також суцільне дотримання політики безпеки об'єкта.

При розробленні політики безпеки необхідно враховувати вимогу збалансувати легкість доступу до інформації і ідентичний механізм ідентифікації дозволеного користувача і забезпечення цілісності та конфіденційності даних. Політика безпеки буде по-справжньому ефективна, якщо вона впроваджується примусово як технічно, так і організаційно.