УДК 004.056.53(045)

Сінько Ю.І., к.пед.н.

ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ ОБМЕЖЕНОГО ДОСТУПУ

Національний авіаційний університет

yusin@ukr.net

Розглянуто деякі питання розробки і організації робіт із забезпечення технічного захисту конфіденційної інформації. Запропоновані визначення, аналіз і класифікація можливих загроз для конкретного об'єкта захисту можуть бути використані фахівцями, які працюють в галузі технічного захисту інформації обмеженого доступу, що не містить відомості, що становлять державну таємницю

Ключові слова: джерело загрози, уразливість, загроза безпеки інформації, атака, несанкціонований доступ до інформації, TCP/IP, sniffer

Постановка проблеми

Одним з основних аспектів проблеми забезпечення безпеки є визначення, аналіз і класифікація можливих загроз для конкретного об'єкта захисту. Перелік найбільш значущих загроз, оцінка ймовірності реалізації загрози і модель зловмисника є базовою інформацією для побудови оптимальної системи захисту.

Основна частина

Аналіз актуальності загроз доцільно проводити на основі логічного ланцюжка: джерело небезпеки – вразливість – загроза – атака.

Джерело загрози – суб'єкт (фізична особа, матеріальний об'єкт або фізичне явище), що є безпосередньою причиною виникнення загрози безпеки інформації [3].

Уразливість – слабкість одного або декількох активів, яка може бути використана однією чи декількома загрозами [3].

Іншими словами вразливість – це слабке місце (пролом) одного з елементів об'єкта захисту, фактор реалізації загрози. Уразливість може бути викликана недоліками процесу експлуатації, властивостями архітектури, недоліками використовуваних протоколів і т. ін.

Загроза безпеки інформації – сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації [3].

Загроза – сукупність умов і факторів, що створюють небезпеку несанкціонованого, в тому числі випадкового, доступу до персональних даних, результатом якого можуть стати знищення, зміна, блокування, копіювання, надання, поширення персональних даних, а також інші неправомірні дії під час їх обробці в інформаційних системах персональних даних (ІСПДн) [3].

Якщо вразливість відповідає загрозі, то існує потенційний ризик.

Атака – спроба реалізації загрози.

Існує безліч критеріїв класифікації загроз. Розглянемо найбільш поширені з них.

1. За природою виникнення: природні та штучні.

Природні загрози – це загрози, викликані впливами на об'єкт захисту і його елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

У свою чергу штучні загрози – це загрози, викликані діяльністю людини.

2. За ступенем впливу на об'єкт захисту: пасивні та активні.

Пасивні загрози – загрози, що не порушують складу і нормальну роботу об'єкта захисту. Приклад – копіювання конфіденційної інформації, витік через технічні канали витоку, підслуховування і т. ін. Активна загроза, відповідно, порушує нормальне функціонування об'єкта захисту, його структуру або склад.

3. Наслідки реалізації загрози – порушення конфіденційності, доступності, цілісності.

До загроз порушення доступності можна віднести як природні, наприклад, пошкодження обладнання через грозу або короткого замикання, так і штучні загрози. Сьогодні широко поширені мережеві атаки на доступність інформації – DDos-атаки.

Останнім часом у спеціальній літературі все частіше йдеться про динамічну та статичну цілісності. До загроз статичної цілісності відноситься незаконна зміна інформації, підробка інформації, а також відмова від авторства. Загрозами динамічної цілісності є порушення атомарності транзакцій, впровадження нелегальних пакетів в інформаційний потік і т. ін.[1].

Також важливо відзначити, що не тільки дані є потенційно вразливими до порушення цілісності, а й програмне середовище. Зараження системи вірусом може стати прикладом реалізації загрози цілісності.

До загроз конфіденційності можна віднести будь-які загрози, пов'язані з незаконним доступом до інформації, наприклад, перехоплення даних, що передаються мережею за допомогою спеціальної програми або неправомірний доступ із використанням підібраного пароля.

4. За способом реалізації: несанкціонований доступ (в тому числі випадковий) до інформації, що захищається, спеціальна дія на інформацію, витік інформації через технічні канали витоку.

Важливо запам'ятати останні дві класифікації загроз, так як саме вони найбільш часто зустрічаються на практиці і в різних нормативних документах.

Класифікація і характеристики загроз безпеки, що пов'язані з несанкціонованим доступом

Несанкціонований доступ до інформації – доступ до інформації, що порушує правила розмежування доступу з використанням штатних засобів, що надаються засобами обчислювальної техніки (ЗОТ) або автоматизованими системами (АС) [3].

Під штатними засобами розуміється сукупність програмного, мікропрограмного і технічного забезпечення засобів обчислювальної техніки або автоматизованих систем. Незважаючи на це, дія впровадженої програмної закладки («хробака» і т. ін.), результатом якої стало попадання інформації, що захищається до зловмисника, також можна розглядати як факт несанкціонованого доступу (НСД).

До основних загроз НСД можна віднести наступне[2]:

- загрози проникнення в операційне середовище комп'ютера з використанням штатного програмного забезпечення (засобів операційної системи або прикладних програм загального використання);
- загрози створення позаштатних режимів роботи програмних (програмно-апаратних) засобів за рахунок навмисних змін службових даних, ігнорування передбачених у штатних умовах обмежень на склад і характеристики оброблюваної інформації, спотворення (модифікації) самих даних і т. ін.;
- загрози впровадження шкідливих програм (програмно-математичного впливу).

Крім цього, можливі комбіновані загрози, що представляють собою поєднання зазначених загроз. Наприклад, за рахунок упровадження шкідливих програм можуть створюватися умови для несанкціонованого доступу в операційне середовище комп'ютера.

Джерелом загроз НСД може бути порушник, носій шкідливої програми, апаратна закладка. Порушники (зловмисники) діляться на внутрішніх і зовнішніх залежно від наявності доступу до інформаційної системи.

Носієм шкідливої програми може бути апаратний елемент комп'ютера (флешка, диск і т. ін.) і програмний контейнер (наприклад, пакети повідомлень, що передаються по комп'ютерній мережі).

Прикладом апаратної закладки може бути апаратний кейлоггер (keelogger). Вони існують в різному виконанні (це

можуть бути моделі, що не вимагають додаткового електроживлення і розміщуватися між клавіатурою і PS/2 портом. Маючи обсяг пам'яті до 2 МВ дозволяє записати понад мільйон символів, введених з клавіатури).

Основні класи атак у мережах на основі TCP/IP

Якщо АС має підключення до мереж загального користування, то можуть бути реалізовані *мережеві атаки* на неї. До мереж загального користування на основі стека протоколів *TCP/IP* відноситься і *Інтернет*, на прикладі якого ми будемо розглядати найбільш поширені сьогодні атаки. Мережа Інтернет створювалася для зв'язку між державними установами та університетом із метою надання допомоги навчальному процесу. На початковому етапі ніхто не міг припустити подальший масштаб його розвитку та інтеграції в життя сучасного суспільства, в зв'язку з чим питанням безпеки не приділялося належної уваги. Як наслідок, сьогодні *стек* має безліч вразливостей, якими з успіхом користуються зловмисники для реалізації атак. Уразливості протоколів, що входять у *стек TCP/IP* обумовлені, як правило, слабкою автентифікацією, обмеженням розміру буфера, відсутністю перевірки коректності службової інформації і т. ін.

Коротка характеристика найбільш небезпечних уразливостей приведена в таблиці 1 [3].

Таблиця 1. Уразливості протоколів стека TCP/IP

Найменування протоколу	**Рівень стека протоколів**	**Найменування (характеристика) уразливості**	**Зміст порушення безпеки інформації**
FTP (*File Transfer Protocol*) – протокол передачі файлів по мережі	Прикладний, представницький, сеансовий	1. Автентифікація на базі відкритого тексту (*паролі пересилаються в незашифрованому вигляді*) 2. Доступ за замовчуванням 3. Наявність двох відкритих портів	Можливість перехоплення даних облікового запису (*імен зареєстрованих користувачів, паролів*). Отримання віддаленого доступу до хостів
Telnet – протокол управління віддаленим терміналом	Прикладний, представницький, сеансовий	Автентифікація на базі відкритого тексту (*паролі пересилаються в незашифрованому вигляді*)	Можливість перехоплення даних облікового запису користувача. Отримання віддаленого доступу до хостів
UDP – протокол передачі даних без встановлення з'єднання	Транспортний	Відсутність механізму запобігання перевантажень буфера	Можливість реалізації UDP-шторму. В результаті обміну пакетами відбувається істотне зниження продуктивності сервера
ARP – протокол перетворення IP-адреси в фізичну адресу	Мережевий	Автентифікація на базі відкритого тексту (*інформація пересилається в незашифрованому вигляді*)	Можливість перехоплення трафіку користувача зловмисником
RIP – протокол маршрутної інформації	Транспортний	Відсутність автентифікації керуючих повідомлень про зміну маршруту	Можливість перенаправлення трафіку через хост зловмисника
TCP – протокол управління передачею	Транспортний	Відсутність механізму перевірки коректності заповнення службових заголовків пакету	Істотне зниження швидкості обміну і навіть повний розрив довільних з'єднань за протоколом TCP

Продовження таблиці 1

DNS – протокол встановлення відповідності мнемонічних імен та мережевих адрес	Прикладний, представницький, сеансовий	Відсутність засобів перевірки автентифікації отриманих даних від джерела	Фальсифікація відповіді DNS-сервера
IGMP – протокол передачі повідомлень про маршрутизації	Мережевий	Відсутність автентифікації повідомлень про зміну параметрів маршруту	Зависання систем Windows
SMTP – протокол забезпечення сервісу доставки повідомлень по електронній пошті	Прикладний, представницький, сеансовий	Відсутність підтримки автентифікації заголовків повідомлень	Можливість підробки повідомлень електронної пошти, а також адреси відправника повідомлення
SNMP – протокол управління маршрутизаторами в мережах	Прикладний, представницький, сеансовий	Відсутність підтримки автентифікації заголовків повідомлень	Можливість переповнення пропускної спроможності мережі

Загрози, що реалізуються через мережу, класифікуються за 6 основними ознаками [4]:

1. Характер загрози.

Пасивна – загроза, яка не впливає на роботу інформаційної системи, але може порушити правила доступу до інформації, що захищається. Приклад: використання sniffer для «прослуховування» мережі. Активна – загроза, яка впливає на компоненти інформаційної системи, під час реалізації якої виявляється безпосередній вплив на роботу системи. Приклад: DDoS-атака у вигляді шторму TCP-запитами.

2. Мета реалізації загрози (відповідно, конфіденційність, доступ-ність, цілісність інформації).

3. Умова початку атаки.

- За запитом того, хто атакує. Тобто зловмисник очікує передачі запиту певного типу, який і буде умовою початку несанкціонованого доступу.
- За настанням очікуваної події на об'єкті, що атакується.
- Безумовний вплив – зловмисник нічого не чекає, тобто загроза реалізується відразу і безвідносно до стану об'єкта, що атакується.

4. Наявність зворотного зв'язку з об'єктом, що атакується:

- Зі зворотним зв'язком, тобто на деякі запити зловмисникові необхідно отримати відповідь. Таким чином, між тим кого атакують і тим, хто атакує є зворотний зв'язок, що дозволяє зловмисникові стежити за станом об'єкта, що атакується і адекватно реагувати на його зміни.
- Без зворотного зв'язку – відповідно, немає зворотного зв'язку і необхідності зловмисникові реагувати на зміни об'єкта, що атакується.

5. Розташування порушника відносно інформаційної системи, що атакується: внутрішньосегментного і міжсегментного. Сегмент мережі – фізичне об'єднання хостів, технічних засобів і інших компонентів мережі, що мають мережеву адресу.

6. Рівень еталонної моделі ISO/OSI, на якій реалізується загроза: фізичний, канальний, мережевий, транспортний, сеансовий, представницький, прикладний.

Розглянемо найбільш поширені сьогодні атаки в мережах на основі стека протоколів TCP/IP [3].

Аналіз мережевого трафіку

Дана атака реалізується за допомогою спеціальної програми, яка називається sniffer. Sniffer являє собою прикладну програму, яка використовує мережеву карту, що працює в режимі promiscuous

mode, так званий «нерозбірливий» режим, в якому мережева плата дозволяє приймати всі пакети незалежно від того кому вони адресовані. У нормальному стані на Ethernet-інтерфейсі використовується фільтрація пакетів канального рівня і якщо MAC-адреса в заголовку призначення прийнятого пакета не збігається з MAC-адресою поточного мережевого інтерфейсу і не є широкомовною, то пакет відкидається. В «нерозбірливому» режимі фільтрація на мережевому інтерфейсі відключається і всі пакети, включаючи не призначені поточному вузлу, пропускаються в систему. Треба зауважити, що багато подібних програм використовуються в легальних цілях, наприклад, для діагностики несправностей або аналізу трафіку. Проте, у розглянутій нами таблиці 1 перераховані протоколи, які відправляють інформацію, в тому числі паролі, в відкритому вигляді – FTP, SMTP, POP3 і т. ін. Таким чином, за допомогою sniffer можна перехопити ім'я і пароль і здійснити несанкціонований доступ до конфіденційної інформації. Більш того, багато користувачів використовують одні й ті ж паролі для доступу до багатьох мережевих сервісів. Тобто, якщо в одному місці мережі є слабкість у вигляді слабкої автентифікації, постраждати може вся мережа. Зловмисники добре знають людські слабкості і широко їх використовують.

Захист від даного виду атаки може полягати в наступному:

• Сильна автентифікація, наприклад, використання одноразових паролів (one-time password). Суть полягає в тому, що пароль можна використовувати одноразово, і навіть якщо зловмисник перехопив його за допомогою sniffer, він не представляє ніякої цінності. Звичайно, даний механізм захисту рятує тільки від перехоплення паролів, і є некорисним у разі перехоплення іншої інформації.

• Анти-сніффери – апаратні або програмні засоби, здатні виявити роботу сніффера в сегменті мережі. Як правило, вони перевіряють навантаження на вузлах мережі з метою визначення «зайвого» навантаження.

• Комутована інфраструктура. Зрозуміло, що аналіз мережевого трафіку можливий тільки всередині одного сегмента мережі. Якщо мережа побудована на пристроях, що розбивають її на велику кількість сегментів (комутатори і маршрутизатори), то атака можлива тільки в тих ділянках мережі, які відносяться до одного з портів даних пристроїв. Це не вирішує проблеми сніффінга, але зменшує межі, які може «прослуховувати» зловмисник.

• Криптографічні методи. Найнадійніший спосіб боротьби з роботою sniffer. Інформація, яка може бути отримана за допомогою перехоплення, є зашифрованою і, відповідно, не має ніякої користі. Найчастіше використовуються IPSec, SSL і SSH.

Сканування мережі

Метою сканування мережі є виявлення працюючих у мережі служб, відкритих портів, активних мережевих сервісів, використовуваних протоколів і т. ін., тобто збір інформації про мережу. Сутність процесу реалізації загрози – передача запитів мережевим службам ІС і аналіз відповідей на них:

• запити DNS допомагають з'ясувати зловмисникові власника домену, адресну область;

• ехо-тестування – виявляє працюючи хости на основі DNS-адрес, отриманих раніше;

• сканування портів – складається повний перелік послуг, що надаються цими хостами, відкриті порти, додатки і т. ін.

Кращим і найбільш поширеним контрзаходом є використання IDS, яка успішно знаходить ознаки ведення сканування мережі та повідомляє про це адміністратора. Повністю позбутися від цієї небезпеки неможливо, так як якщо, наприклад, відключити ехо ICMP і ехо-відповідь на маршрутизаторі, то можна позбутися від загрози ехо-тестування, але

при цьому втратити дані, необхідні для діагностики мережевих збоїв.

Виявлення пароля

Основною метою даної атаки є отримання несанкціонованого доступу до ресурсів, що захищаються шляхом подолання парольного захисту. Щоб отримати пароль, зловмисник може використовувати безліч способів – простий перебір, перебір за словником, сніффінг та ін. Найпоширенішим є простий перебір всіх можливих значень пароля. Для захисту від простого перебору необхідно застосовувати сильні паролі, які не просто підібрати: довжина 6-8 символів, використання букв верхнього та нижнього регістру, використання спеціальних знаків (*@, #, $ і т. ін.*).

Ще однією проблемою інформаційної безпеки є те, що більшість людей використовують однакові паролі до всіх служб, додатків, сайтів тощо. У такому разі вразливість пароля залежить від самої слабкої ділянки його використання.

Подібного роду атак можна уникнути, якщо використовувати одноразові паролі або криптографічну автентифікацію.

IP-spoofing або підміна довіреного об'єкта мережі

Під довіреним в даному випадку розуміється об'єкт мережі (комп'ютер, маршрутизатор, міжмережевий екран і т. ін.), легально підключений до сервера. Загроза полягає в тому, що зловмисник видає себе за довірений об'єкт мережі. Це можна зробити двома способами. По-перше, скористатися IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адрес, або авторизованим зовнішнім адресом, якому дозволяється доступ до певних мережевих ресурсів. Атаки даного типу часто є відправною точкою для інших атак.

Відмова в обслуговуванні

Відмова в обслуговуванні або Denial of Service (DoS) – атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, під час яких легітимні користувачі системи не можуть отримати доступ до надаваних системою ресурсам, або цей доступ ускладнений.

DoS-атака є найбільш поширеною і відомою атакою останнім часом, що зумовлено в першу чергу відносною простотою реалізації. Організація DoS-атаки, як правило, будується на недоліках мережевого програмного забезпечення і мережевих протоколів. Якщо атака проводиться для великої кількості мережевих пристроїв, говорять про розподілену атаку DoS (DDoS – distributed DoS).

Сьогодні найбільш часто використовуються наступні п'ять різновидів DoS-атак, для проведення яких існує велика кількість програмного забезпечення і від яких найважче захиститися:

Smurf - ping-запити ICMP. Під час посилці ping-пакета (повідомлення ICMP ECHO) за широкомовним адресом (наприклад, 10.255.255.255), він доставляється кожній машині в цій мережі. Принцип атаки полягає в посилці пакету ICMP ECHO REQUEST з адресою-джерелом вузла, що атакується. Зловмисник шле постійний потік ping-пакетів за мережевим широкомовним адресом. Всі машини, отримавши запит, відповідають джерелу пакетом ICMP ECHO REPLY. Відповідно, розмір у відповідь потоку пакетів зростає в пропорційне кількості хостів число раз. У результаті, вся мережа наражається на відмову в обслуговуванні через перевантаження.

ICMP flood – атака, аналогічна Smurf, тільки без посилення, що створюється запитами за спрямованим широкомовним адресом.

UDP flood – відправка на адресу вузла, що атакується велику кількість пакетів UDP (User Datagram Protocol) .

TCP flood – відправка на адресу вузла, що атакується велику кількість TCP-пакетів .

TCP SYN flood – під час проведення такого роду атаки видається велика кількість запитів на ініціалізацію TCP-з'єднань з вузлом, що атакується, якому, в результаті, доводиться витрачати всі свої

ресурси на те, щоб відстежувати ці частково відкриті з'єднання.

Якщо ви використовуєте серверний додаток Web-сервер або FTP-сервер, в результаті атаки DoS всі з'єднання, доступні для цих додатків, виявляються зайнятими, і користувачі не можуть отримати до них доступ. Деякі атаки здатні вивести з ладу цілу мережу, наповнивши її непотрібними пакетами. Для протидії таким атакам необхідна участь провайдера, тому що якщо він не зупинить небажаний трафік на вході в мережу, атаку не зупинити, тому що смуга пропускання буде зайнята.

Для ослаблення загрози можна скористатися наступним:

- Функції анти-спіффінга – правильна конфігурація функцій анти-спіффінга на ваших маршрутизаторах і міжмережевих екранах допоможе знизити ризик DoS.
- Функції анти-DoS – правильна конфігурація функцій анти-DoS на маршрутизаторах і міжмережевих екранах може обмежити ефективність атак. Ці функції часто обмежують число напіввідкритих каналів в будь-який момент часу.
- Обмеження обсягу трафіку (traffic rate limiting) – організація може попросити провайдера (ISP) обмежити обсяг трафіку. Цей тип фільтрації дозволяє обмежити обсяг некритичного трафіку, що проходить по вашій мережі. Типовим прикладом є обмеження обсягів трафіку ICMP, який використовується тільки для діагностичних цілей. Атаки DoS часто використовують ICMP [3].

Висновки

Найбільшим за своїм складом ешелоном системи захисту є технічний захист інформації, яка повинна забезпечити цілісність, конфіденційність і доступність інформації, що захищається. Забезпечуючи необхідний рівень захисту інформації, важливо розуміти, що жодна з систем захисту інформації не може забезпечити стовідсотковий захист. Побудова системи захисту це завжди пошук компромісу між витратами на забезпечення інформаційної безпеки, вимог регуляторів і рівнем ризику, який володар інформації готовий прийняти.

Список літератури

1. Зайцев А. П. Технические средства и методы защиты информации. Учебник для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков. Под ред. А. П. Зайцева и А. А. Шелупанова. – 7-е изд., испр. – М.: Горячая линия–Телеком, 2012. – 442 с: ил.

2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации / А.А. Хорев – М.: НПЦ «Аналитика», 2008. - 436 с.: ил.

3. Скрипник Д. Техническая защита информация / Д.Скрипник Электронный ресурс. Режим доступу: https://www.intuit.ru/studies/courses/3649/891/info

4. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев - М. и др. : DiaSoft, 2002. - 671 с. : ил.

5. Блюмин А.М. Мировые информационные ресурсы. Учебное пособие / А.М. Блюмин, Н.А. Феоктистов.- М.: Издательско-торговая корпорация «Дашков и Ко», 2011.-296 с.

Статтю подано до редакції 08.12.2017