# КЛАСИФІКАЦІЯ МЕРЕЖЕВИХ АТАК ТА МЕТОДИ ПРОТИДІЇ І ЗАХИСТУ

*Назар Болехівський, Орест Полотай*
Львівський державний університет безпеки життєдіяльності

**Приведено класифікацію основних мережевих атак. Кожну мережеву атаку розглянуто з точки зору її реалізації та захисту від неї.**
**Ключові слова: комп'ютерна мережа, мережева атака, захист мережі.**

**The classification of major network attacks is given. Each network attack is considered in terms of its implementation and protection against it..**
**Keywords: the computer network, network attack, network protection.**

В реаліях розвитку інформаційного суспільства все більше розвиваються ІТ технології. Комп'ютерні мережі виступають одним з напрямів розвитку суспільства, в якому основним ресурсом виступає інформація. Однак, паралельно з розвитком технологій передачі даних, розвиваються і технології викрадення даних, в тому числі і з комп'ютерної мережі.

Сьогодні існують такі типи мережевих атак:

1. Сніффер пакетів – прикладна програма, яка використовує мережеву карту, що працює в невпорядкованому режимі (в цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатком для обробки). При цьому перехоплюють всі IP-пакети, які передаються через певний сегмент.

Пом'якшити загрозу сніффінга пакетів можна за допомогою таких засобів:

*Аутентифікація*. Сильні засоби аутентифікації є першим способом захисту від сніффінга пакетів. Прикладом є одноразові паролі (OTP - One-Time Passwords). OTP - це технологія двофакторної аутентифікації, при якій відбувається поєднання того, що у вас є, з тим, що ви знаєте. Типовим прикладом двофакторної аутентифікації є робота звичайного банкомату, який пізнає вас, по-перше, по вашій пластиковій картці і, по-друге, по вашому ПІН-коду. Для аутентифікації в системі OTP також потрібно ПІН-код і ваша особиста картка [1].

*Комутована інфраструктура*. Ще одним способом боротьби зі сніффінгом пакетів у вашому мережевому середовищі є створення комутованої інфраструктури. Якщо, наприклад, у всій організації використовується комутований Ethernet, хакери можуть отримати доступ тільки до трафіку, що надходить на той порт, до якого вони підключені (результат микросегментации виробленої комутатором) [1].

*Анти-сніфери*. Третій спосіб боротьби зі сніффінгом полягає в установці апаратних або програмних засобів, які розпізнають сніфери, що працюють у вашій мережі. Ці засоби не можуть повністю ліквідувати загрозу, але, як і багато інших засобів мережевої безпеки, вони включаються в загальну систему захисту.

*Криптографія* – найефективніший спосіб боротьби зі сніффінгом пакетів. Вона робить роботу сніфферів марною.

2. IP-спуфінг відбувається, коли хакер, що знаходиться всередині корпорації або поза нею, видає себе за санкціонованого користувача. Це можна зробити двома способами. По-перше, хакер може скористатися IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адрес, або вповноваженою зовнішньою адресою, якому дозволяється доступ до певних мережевих ресурсів.

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

*Контроль доступу* – найпростіший спосіб запобігання IP-спуфінга. Він полягає в правильному підборі управління доступом. Щоб знизити ефективність IP-спуфінга, необхідно відсікти будь-який трафік, що надходить із зовнішньої мережі.

*Фільтрація RFC 2827*. Можна припинити спроби спуфінга чужих мереж користувачами нашої мережі (і стати добропорядним «мережевим громадянином»). Для цього необхідно

блокувати будь-який вихідний трафік, адреса джерела якого не є однією з IP-адрес нашої організації.

*Аутентифікація*. IP-спуфинг може функціонувати тільки за умови, якщо аутентифікація відбувається на базі IP-адрес. Тому впровадження додаткових методів аутентифікації робить цей вид атак марним.

3. Парольні атаки. Хакери можуть проводити парольні атаки за допомогою цілого ряду методів, таких як простий перебір (brute force attack), «троянський кінь», IP-спуфінг і сніффінг пакетів.

Парольних атак можна уникнути, якщо не користуватися паролями в текстовій формі. Одноразові паролі і / або криптографічна аутентифікація можуть практично звести нанівець загрозу таких атак.

З точки зору адміністратора, існує кілька методів боротьби з підбором паролів. Один з них полягає у використанні засоби L0phtCrack, яке часто застосовують хакери для підбору паролів в середовищі Windows NT. Це засіб швидко покаже вам, чи легко підібрати пароль, вибраний користувачем [2].

4. Атаки на рівні додатків можуть проводитися кількома способами. Найпоширеніший з них полягає у використанні добре відомих слабкостей серверного програмного забезпечення (sendmail, HTTP, FTP). Використовуючи їх, хакери можуть отримати доступ до комп'ютера від імені користувача, що працює з додатком. Відомості про атаки на рівні додатків широко публікуються, щоб дати можливість адміністраторам виправити проблему за допомогою корекційних модулів (патчів). На жаль, багато хакерів також мають доступ до цих відомостей, що дозволяє їм вчитися [3].

5. Мережевою розвідкою називається збір інформації про мережу за допомогою загальнодоступних даних і додатків. При підготовці атаки проти будь-якої мережі хакер, як правило, намагається отримати про неї якомога більше інформації. Мережева розвідка проводиться у формі запитів DNS, exo-тестування (ping sweep) і сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цього домену привласнені. Exo-тестування (ping sweep) адрес, розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють в даному середовищі. Отримавши список хостів, хакер використовує засоби сканування портів, щоб скласти повний список послуг, що надаються цими хостами. І, нарешті, хакер аналізує характеристики додатків, що працюють на хостах. В результаті видобувається інформація, яку можна використовувати для злому.

Повністю позбавитися від мережевої розвідки неможливо.

6. Соціальна інженерія. Часто, проектуючи мережеву безпеку, забувають захиститися від одного з найпростіших і в той же час дієвих способів злому – соціальної інженерії. Вона заснована на роботі зі службовцями компанії, їх підкуп або введення в оману. Наприклад, хакер може зателефонувати службовцю і, видавши себе за мережевого адміністратора, попросити назвати свій пароль для виконання будь-яких дій.

Протидія таким методам може здійснюватися лише через навчання і підготовку персоналу, закріплення в політиці безпеки правил поведінки.

Це далеко не повний вид мережевих атак, що розвинулись за останні декілька років. Аналітику безпеки чи системному адміністратору необхідно володіти всіма способами захисту від приведених вище атак ат вміти їх ефективно застосовувати на практиці.

**Література**

1. Веб-сайт beasthackerz. [Електронний ресурс]. Режим доступу з beasthackerz.ru/uk/kompyuter/vidy-atak-identifikac...irovanie-portov.html

2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч. закл., які навчаються за напрямами "Безпека інформаційних і комунікаційних систем", "Системи технічного захисту інформації", "Управління інформаційною безпекою" / М. В. Грайворонський, О. М. Новіков. – К. : Вид-во BHV, 2009. – 608 с.

3. Петров В.А. Інформаційна безпека. Захист інформації від несанкціонованого доступу в автоматизованих системах / Петров В.А., Піскарьов С.А., Шеїн А.В. – М. : Изд-во Ореан, 1998. – 534 с.