***Ейсмонт О.С., магістрант,***
***Грабар О.І., к.т.н., доц.,***
*Житомирський державний технологічний університет*

# ЗАХИСТ МЕРЕЖІ ВІД SPOOFING

Забезпечення мережевого захисту – одне з найскладніших завдань у сфері захисту інформаційних систем. Більшість сучасних систем має розподілену структуру, в основі їх архітектури лежить використання мережевих технологій. Забезпечення працездатності таких систем залежить від здатності протистояти зловмисним діям, які спрямовані на порушення роботи як самої мережі, так і інформаційної системи, що функціонує в її рамках. Одними з найбільш небезпечних видів злочинної діяльності в мережі Інтернет є так звані мережеві атаки. Як свідчить статистика, наведена в Інтернет–джерелах, кількість мережевих атак продовжує зростати, методи, якими користуються злочинці, постійно розвиваються і удосконалюються, від одиничних спроб вони переходять до корпоративних розробок. У той же час сучасні системи виявлення вторгнень і атак ще не досконалі і недостатньо ефективні з точки зору безпеки рішень. Тому методи роботи в цьому напрямку необхідні і актуальні.

Одними з таких атак є Spoofing-атаки. Spoofing - загальна назва для мережевих атак, коли один учасник маскується під іншого. Багато з протоколів в TCP / IP не забезпечують механізми для аутентифікації джерела чи призначення повідомлення. Таким чином, вони уразливі для спуфинга, якщо тільки додатками не будуть прийняті додаткові заходи безпеки для ідентифікації відправника і одержувача. IP-спуфинг і ARP спуфинг зокрема можуть використовуватися для атак «людина посередині» на хости в комп'ютерній мережі. Захист від спуфинг атак може бути збільшена з використанням брандмауерів, здатних до глибокої інспекції пакетів, або шляхом вжиття заходів з перевірки особистості відправника або одержувача повідомлення.

Поширені spoofing-атаки:

- MAC-spoofing - атака канального рівня, що полягає в тому, що на мережевій карті змінюється MAC-адресу, що змушує комутатор відправляти на порт, до якого підключений зловмисник, пакети, які до цього він бачити не міг;
- ARP-spoofing - атака, експлуатуюча слабкість протоколу ARP, що дозволяє розмістити в ARP-кеші жертви неправдивий запис про відповідність IP-адреси іншої жертви MAC-адресою атакуючого;
- IP-spoofing - атака, яка полягає у використанні в IP-пакетів, що відправляються жертві, IP-адрес хоста, якому вона довіряє; легко здійсненна в UDP, в деяких випадках можлива в TCP-судинних;
- DNS-spoofing - атака, що базується на зараженні кеша DNS-сервера жертви помилковим записом про відповідність DNS-імені хоста, якому жертва довіряє, і IP-адреси атакуючого.

Spoofing в телефонних мережах загального користування можна дізнатися, хто вам телефонує, дивлячись на інформацію про абонента, яка передається з викликом. Є технології, які передають цю інформацію на стаціонарні телефони, на мобільні телефони, а також з VoIP. В даний час з'явилися технології, які дозволяють абонентам передавати помилковий ідентифікатор і представляти помилкові імена і номери, які, звичайно, можуть бути використані в недобросовісних цілях.

Spoofing E-mail - інформацію про відправника, показану в електронній пошті можна легко підробити. Цей метод зазвичай використовується спамерами, щоб приховати походження своєї електронної пошти і призводить до таких проблем, як повернуті листи (тобто спаму в електронній пошті зворотного розсіювання).

Spoofing атака на GPS - атака, яка намагається обдурити GPS-приймач, широкомовно передаючи трохи більш потужний сигнал, ніж отриманий від супутників GPS, такий, щоб бути схожим на ряд нормальних сигналів GPS. Ці імітують сигнали змінені таким способом, щоб змусити одержувача не визначити своє місце розташування, вважаючи його таким, яке відправить атакуючий. Оскільки системи GPS працюють вимірюючи час, який потрібен для сигналу, щоб дійти від супутника до одержувача, успішний спуфинг вимагає, щоб атакуючий точно знав, де його мета - так, щоб імітує сигнал міг бути структурований з належними затримками сигналу.

В більшості своїй spoofing-атаки спрямовані на те, щоб змусити жертву відправляти трафік не легітимному одержувачу безпосередньо, а атакуючому, який потім вже ретранслює трафік далі. При цьому атакуючий отримує можливість модифікації трафіку або, як мінімум, перегляду. У разі IP-spoofing'а переслідується інша мета - змусити жертву повірити, що трафік приходить від легітимного відправника і повірити йому.

У наші дні значна увага приділяється зовнішнім атакам, а питання внутрішньої безпеки нажаль обходять стороною. Ця неувага до захисту від зловмисників залишає непогані шанси проведення локальних атак. Що стосується атак на додатки, то у них попереду велике майбутнє через зростання складності мережевих додатків і зменшення термінів розробки програмних проектів. Все це веде до збільшення кількості помилок в коді. Атаки на відмову в обладнанні залишатимуться у своїй формі, поки користувачі не усвідомлять необхідність захищати свої власні комп’ютери.