УДК 004.415.2
DOI https://doi.org/10.32782/2663-5941/2023.4/16

Поліщук С.М.
Український науково-дослідний інститут спеціальної техніки
та судових експертиз Служби безпеки України

ЛАНДШАФТ ЗАГРОЗ СПУФІНГУ: ТЕНДЕНЦІЇ, ВРАЗЛИВОСТІ ТА НАПРЯМКИ ДОСЛІДЖЕНЬ

Ця стаття має на меті привернути увагу студентів, користувачів комп'ютерів і дослідників-початківців до такого типу небезпеки, як спуфінг. Спуфінг передбачає видавання себе за когось іншого або за комп'ютер шляхом надання неправдивої інформації, такої як імена електронної пошти, URL-адреси чи IP-адреси. Комп'ютерний світ представляє різні форми спуфінгу, усі вони маніпулюють інформацією за допомогою оманливих засобів.У цій статті розглядається наступні типи спуфінгу: IP, ARP, E-Mail, Web і DNS. Важливо зазначити, що будь-яка форма спуфінгу не використовується законно чи конструктивно. Наслідки таких атак можуть бути жахливими, призводячи до мільйонних фінансових втрат, а також до потенційної шкоди окремим особам і організаціям. IP-спуфінг передбачає маніпулювання IP-адресами, щоб змусити системи довіряти джерелу даних. З іншого боку, ARP-спуфінг використовує протокол розпізнавання адрес, щоб зв'язати MAC-адресу зловмисника з законною IP-адресою. Підробка електронної пошти обманює одержувачів, змінюючи адресу відправника так, щоб вона виглядала неначе її відправлено кимось іншим. Веб-спуфінг створює підроблені веб-сайти, які імітують законні веб-сайти, щоб викрасти конфіденційну інформацію. Нарешті, підробка DNS перенаправляє користувачів на шкідливі веб-сайти, змінюючи записи DNS. Щоб захиститися від атак спуфінгу, слід застосувати кілька заходів виявлення та запобігання. Впровадження надійних механізмів автентифікації може допомогти перевірити ідентичність користувачів і систем. Розширені методи шифрування, такі як цифрові підписи та сертифікати SSL, можуть захистити цілісність даних під час передачі. Адміністратори мережі повинні відстежувати мережевий трафік і шукати нерегулярні шаблони, які можуть вказувати на спроби підробки. Крім того, розгортання систем виявлення вторгнень (IDS) і систем запобігання вторгненням (IPS) може допомогти виявляти та блокувати атаки підробки в реальному часі. Для додавання додаткового рівня безпеки та забезпечення цілісності даних DNS можна використовувати DNSSEC (Domain Name System Security Extensions). Навчання користувачів щодо спуфінгу та сприяння пильності під час роботи з електронними листами та веб-сайтами також може значно знизити ризик стати жертвою таких атак. А регулярні тренінги з питань безпеки можуть допомогти користувачам виявляти підозрілі дії та негайно повідомляти про них. Слід зазначити, що розуміння різних типів атак спуфінгу має важливе значення для захисту цифрових активів і особистої інформації. Ознайомившись із методами виявлення та запобігання до таких типів атак, можливо мінімізувати руйнівні наслідки спуфінгу, як для окремих осіб, так і для організацій.

Ключові слова: *спуфінг, кіберзахист, атаки, IP спуфінг, ARP спуфінг, E-Mail спуфінг, Web спуфінг, DNS спуфінг.*

Постановка проблеми. Глобальні обчислення за допомогою розумних пристроїв стали звичним явищем, покращуючи якість життя. Але з'явилися і ризики для безпеки. Глобальне середовище залежить від підключених мереж, що робить мережеву безпеку життєво важливою. Захист цих мереж має вирішальне значення. Одним із видів загроз в глобальній мережі є спуфінг. Атаки спуфінгу є одними з найпоширеніших атак у мережі і використовують метод за допомогою якого кіберзлочинці видають себе за: відоме або надійне джерело інформації, за людину або систему. Спуфінг може приймати різноманітні форми:

– IP: підробка IP-адреси джерела, щоб замаскувати відправника;

– ARP: пов'язує MAC-адресу зловмисника з цільовою IP-адресою;

– електронна пошта: Підробляє заголовки, щоб імітувати відправника;

– веб: копіює сайти для викрадення облікових даних;

– DNS: перенаправляє трафік через пошкоджені дані.

Спуфінг має лише зловмисні цілі, такі як крадіжка або завдання шкоди. Атаки можуть серйозно пошкодити системи і коштувати мільйони. Система безпеки повинна відстежувати та запобігати спуфінгу, враховуючи серйозну загрозу, яку він становить, оскільки комп'ютерні технології стають все більш поширеними.

Аналіз останніх досліджень і публікацій. Зловмисники використовують різноманітні типи спуфінгових атак, але найбільшого поширення серед них набули такі типи спуфінгу: IP, ARP, E-Mail, Web і DNS. Підміна IP-адреси полягає у видаванні себе за довірену систему для отримання несанкціонованого доступу. Зловмисники надсилають пакети на ціль з підробленими адресами джерела, створюючи враження, що вони надходять з довіреного порту або пристрою [1]. Такі дії можливі оскільки системи функціонують у групах інших «довірених» систем та реалізується шляхом автентифікації за IP-адресою із-за погано налаштованих маршрутизаторів у випадку надходження пакетів з зовнішніх джерел [2]. Зокрема у дослідженнях зазначається такий тип спуфінгу, як ARP (Address Resolution Protocol) спуфінг. Протокол ARP зіставляє IP-адреси з MAC-адресами і зберігає ці пари в кеші [3, с. 48]. Термін дії записів закінчується через 20 хвилин. Коли хосту потрібен MAC-адреса для IP-адреси, він надсилає ARP-запит. Хост з цим IP/MAC відповідає своєю інформацією, щоб ARP міг оновити кеш відправника [4, с. 22; 5, с. 3866]. Однак, ARP не має автентифікації, що уможливлює атаки з підміною ARP [6, с. 1]:

1. блокування – зловмисник отруює кеш, щоб перенаправляти пакети не за призначенням;

2. видавання себе за жертву – зловмисник асоціює свій MAC-адрес з IP-адресою жертви для відкидання пакетів;

3. man-in-the-middle – зловмисник асоціює себе між двома хостами для перехоплення зв'язку.

Але недоліки аутентифікації роблять протокол ARP вразливим до атак підміни.

Іншим видом загрози є підробка електронної пошти відомий, як спуфінг електронної пошти – E-mail спуфінг [7, с. 27]. Спуфінг електронної пошти може сприяти зловмисним діям, включаючи розповсюдження вірусів, фішинг для отримання конфіденційної інформації, крадіжку корпоративних даних та інші форми кібершпигунства. Небезпеку становить і підробка URL-адрес, що передбачає створення підроблених веб-сайтів, які видають себе за легітимні, з метою крадіжки інформації про користувачів або розповсюдження шкідливого програмного забезпечення [8].

Натомість DNS (Domain Name System) спуфінг небезпечний тим, що зловмисники використовують вразливості в програмному забезпеченні DNS-серверів або застосовують соціальну інженерію для вставки фальшивих записів. Це дозволяє їм перенаправляти користувачів на підконтрольні зловмисникам сайти, що видають себе за справжні домени [9, с. 84].

Незважаючи на значну кількість наукових публікацій, присвячених проблемам захищеності від спуфінг атак, існує потреба у подальших дослідженнях цієї тематики.

Метою статті є всебічний аналіз і цілеспрямоване дослідження проблем кібербезпеки, пов'язаних з такими типами атак, як спуфінг. Розглядаються наступні типи спуфінгу: IP, ARP, E-Mail, Web і DNS. Важливо зазначити, що будь-яка форма спуфінгу не використовується законно чи конструктивно. Наслідки таких атак можуть бути жахливими, призводячи до мільйонних фінансових втрат, а також до потенційної шкоди окремим особам і організаціям.

Виклад основного матеріалу дослідження. Спуфінг – це небезпечна практика фальсифікації даних в комп'ютерних мережах, що включає різноманітні методи фальсифікації інформації. На практиці найбільш поширені такі основні типи кібератак з використанням спуфінгу:

– підробка IP-адреси для приховування дійсного джерела трафіку;

– ARP спуфінг для перехоплення мережевих пакетів шляхом асоціації чужого MAC адресу зі своєю IP;

– підробка електронної пошти – створення листів від імені інших користувачів;

– веб-спуфінг – копіювання сайтів для крадіжки даних;

– підміна DNS для перенаправлення трафіку на шкідливі ресурси.

Спуфінг не має жодного законного застосування, використовується виключно зі злочинною метою та може завдати серйозних фінансових збитків і репутаційних втрат. Захист від спуфінгу потребує комплексного підходу і постійної уваги фахівців кібербезпеки.

Підміна IP-адреси є одним з найбільш поширених методів кібератаки, який використовують зловмисники для отримання неавторизованого доступу до комп'ютерних систем та мереж. Суть цієї атаки полягає в надсиланні на цільовий пристрій шкідливих мережевих пакетів з підробленою IP-адресою джерела, що створює хибне враження, ніби пакети надходять з надійного, довіреного вузла мережі [1]. Для успішного здійснення підміни IP зловмиснику необхідно виконати низку складних технічних кроків:

– ідентифікувати цільову систему та отримати її мережеві параметри;

– знайти IP-адресу якогось надійного вузла в цій мережі, наприклад маршрутизатора;

– якимось чином відключити реальний зв'язок з довіреним вузлом, щоб перехопити трафік;

– перехопити зразок комунікації між ціллю та надійним хостом;

– підібрати порядкові номери пакетів, що використовує довірений вузол;

– змінити заголовки пакетів так, щоб вони здавалися такими, ніби надійшли з довіреного хоста;

– спробувати несанкціоноване підключення до сервісу, який вимагає автентифікації.

Основна мета підміни IP – видати себе за одну систему (B), використовуючи IP-адресу іншої довіреної системи в мережі (A). Це можливо тому, що вузли часто довіряють іншим вузлам всередині локальної мережі або сегмента. Недолік полягає в тому, що атака є «сліпою» без зворотного зв'язку. Для успіху потрібні досвід та знання мереж.

Для запобігання підміни IP слід використовувати автентифікацію IP, фільтрацію трафіку, моніторинг, вимикати непотрібну маршрутизацію пакетів. Це складна, але небезпечна атака, яка потребує постійної уваги фахівців кібербезпеки.

Протокол ARP відповідає за встановлення відповідності між IP-адресами та фізичними MAC-адресами пристроїв в мережі [2]. Він використовує ARP-кеш – таблицю, що зберігає співставлення MAC і IP адрес. Коли маршрутизатор отримує пакет для хоста в мережі, він звертається до ARP, щоб знайти MAC-адресу за відомою IP. Якщо запис є в ARP-кеші – повертається MAC і пакет надсилається за цією адресою. Інакше ARP розсилає запит на всі хости мережі, щоб знайти MAC для IP. Комп'ютер, що розпізнає свою IP, відповідає своєю MAC. ARP оновлює кеш і надсилає пакет за отриманою MAC-адресою. Підміна ARP полягає у надсиланні фальшивих ARP-запитів і відповідей для отримання неправдивих співставлень MAC та IP адрес. Це дозволяє зловмиснику перенаправляти трафік з одного пристрою на інший. Існують утиліти для автоматизації ARP спуфінгу, що спрощує перехоплення пакетів та MITM-атаки.

Для запобігання підміні ARP є два основні методи. По-перше, прив'язка MAC-адрес на комутаторі, що унеможливлює зміну вже призначеного MAC. По-друге, використання статичних ARP-таблиць, хоча це можливо лише в невеликих мережах. Додатково для виявлення змін в ARP-кеші можна застосовувати моніторинг, наприклад, утиліту ARPWatch в UNIX-системах. Це допомагає оперативно реагувати на спроби атак підміни ARP.

ARP спуфінг є поширеною загрозою, що дозволяє перехоплювати трафік в локальних мережах. Слід впроваджувати заходи для запобігання та виявлення таких атак, зокрема, обмеження динамічної зміни ARP-таблиць, моніторинг, аутентифікація. Безпека ARP має критичне значення для захисту внутрішніх мереж від несанкціонованого доступу.

Підробка електронної пошти є поширеною кіберзагрозою, що полягає у надсиланні повідомлень, котрі видаються такими, ніби надійшли від легітимного джерела, проте насправді є фальшивками від зловмисників. Метою такої підробки зазвичай є здійснення шахрайських, злочинних або шкідливих дій, зокрема: поширення вірусів та шкідливого програмного забезпечення, фішинг конфіденційних даних, промислове шпигунство, крадіжка грошей тощо. Як і в звичайних поштових листах, в електронних повідомленнях містяться зворотні адреси відправників, котрі досить легко підробити за допомогою спеціальних засобів [7, с. 27]. Найпоширеніші причини для здійснення спуфінгу електронної пошти:

– обхід антиспам законодавства та уникнення юридичної відповідальності за розсилку незаконного спаму;

– приховування авторства листів з погрозами, переслідуванням чи шантажем;

– спонукання користувачів відкрити шкідливі вкладення, видаючи лист за повідомлення від знайомого джерела;

– соціальна інженерія – видавання себе за довірену особу з метою виманити конфіденційні дані;

– завдання репутаційної шкоди іншим особам шляхом створення фальшивих листів від їхнього імені.

Ефективний захист від підробки електронної пошти вимагає комплексу технічних і організаційних заходів, зокрема: фільтрації спаму, перевірки заголовків листів, впровадження DMARC (Domain-based Message Authentication, Reporting and Conformance), обережності при відкритті вкладень у листах, навчання користувачів тощо.

Метою такого типу кібератаки, як веб-спуфінг – є введення в оману користувачів шляхом надання їм неправдивої інформації. При цій атаці зловмисник може переглядати та маніпулювати веб-сторінками, що надсилаються на пристрій жертви, отримуючи доступ до введених нею даних у формах [8]. Це становить значний ризик компрометації конфіденційної інформації, такої як адреси, номери карток, банківські реквізити та паролі. Веб-спуфінг реалізується в браузерах IE, Netscape та інш. і може обійти захищене SSL-з'єднання. Незважаючи на індикацію безпечного зв'язку, зловмисник може стежити за сторінками і маніпулювати ними, а також

перехоплювати відправлені дані. Атака складається з двох частин. По-перше, створення підробленого браузерного вікна на пристрої жертви із заміною окремих компонентів. По-друге, перенаправлення всіх сторінок через сервер зловмисника, де вони непомітно модифікуються. Таким чином користувачі можуть потрапити на шкідливі сторінки або листи. Сучасні браузери не повністю захищені від веб-спуфінгу, що створює серйозні перешкоди для безпечної електронної комерції.

Для захисту від веб-спуфінгу потрібно регулярно оновлювати програмне забезпечення, використовувати надійні браузери, уникати підозрілих посилань, застосовувати VPN (virtual private network) та інші засоби кібербезпеки. Подолання вразливостей вебспуфінгу критично важливе для забезпечення цілісності та безпеки онлайн-транзакцій.

Ще одна найбільш часто поширена кібератака – підміна DNS, що полягає у несанкціонованому внесенні хостом неправдивої інформації про DNS-розв'язання, внаслідок чого користувачі перенаправляються на шкідливі сайти [9, с. 84]. Зловмисники використовують соціальну інженерію або користуються вразливостями програмного забезпечення DNS-серверів, щоб змінювати DNS-записи та вводити в оману користувачів. Перенаправивши користувача на підконтрольний сайт, зловмисник може виконати атаку «людина посередині» та викрасти конфіденційні дані. За звичайних умов корчувач очікує отримати зі свого DNS-серверу правильну IP-адресу ресурсу. Проте під час атаки підміни DNS зловмисник змінює запис для потрібного хоста, підмінюючи справжню IP-адресу на фальшиву. Коли клієнт звертається до скомпрометованого DNS, він отримує сфальсифіковану відповідь та переходить на небезпечний сайт замість легітимного ресурсу.

Для захисту критично важливо забезпечити безпеку DNS-інфраструктури, регулярно оновлювати програмне забезпечення, використовувати DNSSEC (Domain Name System Security Extensions), моніторити трафік, застосовувати брандмауери та інші засоби кібербезпеки.

Висновки. Запобігання атакам спуфінгу вкрай важливе для підтримки безпеки мережі. Існують ефективні методи фільтрації пакетів:

– метод фільтрації на вході (IFM – Ingress Filtering Method) перевіряє автентичність вхідних пакетів на основі IP-адреси джерела. Проте цей метод обмежений для мереж з одним підключенням;

– метод фільтрації на виході (EFM – Egress Filtering Method) контролює вихідний трафік, фільтруючи пакети за політиками безпеки. EFM допомагає запобігти несанкціонованому трафіку;

– метод запобігання підмінам (SPM – Spoofing Prevention Method) використовує унікальний ключ між джерелом і одержувачем для автентифікації. SPM дозволяє поетапне розгортання.

Для веб-додатків можна застосувати:

– криптографічні підписи для автентифікації повідомлень;

– налаштування демонів доставки пошти для блокування спуфінгу;

– логування для відстеження джерела спуфінгу;

– централізований поштовий хаб як єдину точку входу.

– нформування користувачів для запобігання соціальній інженерії.

Ці методи в комплексі значно знижують ризики спуфінг-атак. Крім того, фахівцям кібербезпеки важливо розуміти серйозність загрози та оперативно лагодити вразливості. Потрібні постійний моніторинг і навчання, адже зловмисники наполегливо шукають слабкі місця. Захист від нових видів атак вимагає гнучкості та адаптації. Комплексний підхід до безпеки – запорука успіху в боротьбі зі спуфінгом та підтримання довіри користувачів.

Список літератури:

1. Daemon, Route, Infinity, «IP Spoofing Demystified», Phrack Magazine, vol. 7 issue 48, 1996.

2. «IP Address Spoofing and Hijacked Session Attacks»; 1/23/95 http://ciac.llnl.gov/ciac/bulletins/f-08.shtml.

3. R. Philip, Securing wireless networks from ARP cache poisoning [M.S. thesis], San Jose State University, 2007, p. 48.

4. C. L. Abad and R. I. Bonilla, «An analysis on the schemes for detecting and preventing ARP cache poisoning attacks,» in Proceeding of the 27th International Conference on Distributed Computing Systems Workshops (ICDCSW '07), Toronto, Canada, June 2007, pp. 22–29.

5. S. Y. Nam, S. Djuraev, and M. Park, «Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks,» Computer Networks, vol. 57, 2013, pp. 3866–3884.

6. L. Wu, T. Yu, D. Wu, and J. Cheng, «The Research and Implementation of ARP Monitoring and Protection,» in Proceedings of the International Conference on Internet Technology and Applications (iTAP '11), Wuhan, China, August 2011, pp. 1–4.

7. Rajinder Kumar, Amandeep Jindal and Kunal Pandove. Article: Email Spoofing. International Journal of Computer Applications 5(1), August 2010. Published By Foundation of Computer Science, pp. 27–30.

8. Felten, Balfanz, Dean, Wallach D.S., «Web Spoofing, An Internet Con Game»; http://bau2.uibk.ac.at/matic/spoofing.htm

9. Maksutov A.A., Cherepanov I.A., Alekseev M.S. Detection and prevention of DNS spoofing attacks. In Siberian symposium on data science and engineering., IEEE. 2017, pp. 84–91.

Polischuk S.M. THE SPOOFING THREAT LANDSCAPE: TRENDS, VULNERABILITIES AND FUTURE RESEARCH DIRECTION

This article aims to make students, computer users, and novice researchers aware of the dangers of spoofing. Spoofing involves pretending to be someone else or a computer by providing false information such as email names, URLs, or IP addresses. The computer world presents various forms of spoofing, all of which manipulate information through deceptive means. This article covers the following types of spoofing: IP, ARP, E-Mail, Web, and DNS. It is important to note that any form of spoofing is not used legally or constructively. The consequences of such attacks can be dire, leading to millions of dollars in financial losses, as well as some harm to individuals and organizations. IP spoofing involves manipulating IP addresses to trick systems into trusting data sources. ARP spoofing, on the other hand, uses the Address Resolution Protocol to associate an attacker's MAC address with a legitimate IP address. E-mail phishing tricks recipients by changing the sender's address to make it look like it was sent by someone else. Web spoofing creates fake websites that mimic legitimate websites in order to hide sensitive information. Finally, DNS spoofing redirects users to malicious websites by altering DNS records. Several detection and prevention measures should be implemented to protect against spoofing attacks. Implementing strong authentication mechanisms can help verify the identity of users and systems. Advanced encryption methods, such as digital signatures and SSL certificates, can protect the integrity of data in transit. Network administrators should monitor network traffic and look for irregular patterns that may indicate spoofing attempts. In addition, deploying intrusion detection systems (IDS) and intrusion prevention systems (IPS) can help detect and block spoofing attacks in real time. DNSSEC (Domain Name System Security Extensions) can be used to add an additional layer of security and ensure the integrity of DNS data. Educating users about spoofing and promoting vigilance when dealing with emails and websites can also significantly reduce the risk of falling victim to such attacks. And regular security training can help users spot suspicious activity and report it immediately. It should be noted that understanding the different types of spoofing attacks is essential to protecting digital assets and personal information. By learning how to detect and prevent these types of attacks, it is possible to minimize the devastating effects of spoofing, both for individuals and organizations.

Key words: *spoofing, cyber protection, attacks, IP spoofing, ARP spoofing, E-Mail spoofing, Web spoofing, DNS spoofing.*