Тези доповідей 54-ї наукової конференції молодих дослідників ОНПУ-магістрантів «Сучасні інформаційні технології та телекомунікаційні мережі» // Одеса: ОНПУ, 2019, вип.54

# ЗАГРОЗИ МЕРЕЖЕВОЇ БЕЗПЕКИ ТА МОДЕЛІ ЇЇ ЗАХИСТУ

# УГРОЗЫ СЕТЕВОЙ БЕЗОПАСНОСТИ И МОДЕЛИ ЕЕ ЗАЩИТЫ

# NETWORK SECURITY THREATS AND ITS PROTECTION MODELS

Науковий керівник – доцент кафедри радіотехнічних пристроїв
Агаджанян А.Р., Агаджанян А.Р., Agadzanyan A.
Виконала – Потоцька К.В., Потоцкая Е.В., Pototska K.

**Анотація:** були розглянуті основні види загроз мережевої безпеки та розроблена модель захисту мережі.

**Ключові слова:** флудинг, кейлогер, троянська програма, блютуз-атака, фішиг, сніфер, атака нульового дня.

**Аннотация:** были рассмотрены основные виды угроз сетевой безопасности и разработана модель защиты сети.

**Ключевые слова:** флудинг, кейлоггер, троянская программа, блютуз-атака, фишинг, сниффер, атака нулевого дня.

**Abstract:** the main types of network security threats were considered and a network protection model was developed.

**Key words:** flooding, keylogger, Trojan, Bluetooth-attack, phishing, sniffer, Zero-day attack.

Питання мережевої безпеки є актуальним, оскільки заходи з її забезпечення  означають зручність, надійність та безпеку інфраструктури та даних мережі. Ефективна мережева безпека зосереджується на різноманітних загрозах і перешкоджає їх проникненню чи поширенню у мережу. Серед найбільш поширених загроз виділяють:

– флудинг (алгоритм маршрутизації, в якому кожний наступний вхідний пакет надсилається через кожне вихідне посилання, крім того, на яке він надійшов);

– кейлогери (програмне забезпечення, що реєструє різноманітні дії користувача – натискання клавіш на клавіатурі комп'ютера, рухи та натискання клавіш миші та ін.);

– троянські програми (зловмисне програмне забезпечення, що вводить користувачів в оману щодо його намірів);

– блютуз-атаки (блюджекінг, блюснарфінг, блюбаггінг);

– фішинг (вид інтернет-шахрайства, спрямований на отримання доступу до конфіденційних даних користувача – логінів та паролів);

– заглушення сигналу (навмесне заглушення, блокування чи перешкоджання дозволеному бездротовому зв'язку);

– сніферні атаки (крадіжка або перехоплення даних шляхом захоплення мережевого трафіку);

– скомпрометовані сервери (захоплення северу для використання з власною ціллю);

– діри в серверній безпеці (найбільші уразливості системи безпеки);

– атаки нульового дня (ще невідомі та неліквідовані уразливості, а також шкідливі програми, проти яких ще не розроблені механізми захисту).

На основі досліджених загроз запроновано модель захисту мережі від несанкціонованого доступу.

Необхідне налаштування профілю, який забезпечує захист від флудингу від пакетів SYN, ICMP, ICMPv6 та UDP, а також інших типів IP-пакетів. Для цього треба вказати поріг повідомлення – кількість запитів з однієї IP-адреси, після яких відбувається запис в журнал, і поріг відкидання пакетів – кількість запитів, після яких пакети відкидаються з відповідним записом у журналі.

Методами захисту від несанкціоновано установлених кейлогерів є використання антишпигунських програмних продуктів та/або антивірусних програм, використання програм, які шифрують дані, що вводяться з клавіатури, використання віртуальних клавіатур.

Троянські програми виявляються та видаляються антивірусним та антишпигунським програмним забезпеченням, як і більшість шкідливих програм.

Для захисту від фішингу необхідно завжди перевіряти URL-адресу, за якою рекомендується перейти, на наявність незначних помилок, використовувати лише безпечні https-з’єднання, за можливості на всіх аккаунтах підключити двофакторну аутентифікацію.

Щоб захиститися від сніферу треба шифрувати всю інформацію, що приймається та відправляється, сканувати свою локальну мережу на наявність уразливостей, використовувати тільки перевірені та захищені мережі Wi-Fi.

У зв'язку із застосуванням спеціальних технологій, загрози нульового дня не можуть бути виявленими класичними антивірусними технологіями. На думку антивірусних компаній, для забезпечення ефективного захисту проти таких шкідливих програм і вразливостей потрібно використовувати проактивні технології антивірусного захисту.

Проведений аналіз дозволив виявити ключові компоненти мережевої безпеки, а саме:

– антивірусне програмне забезпечення, що своєчасно оновлюється;

– брандмауер, який блокує несанкціонований доступ до персонального комп’ютеру на робочих станціях (USB-порти, LAN, Wi-Fi);

– віртуальні приватні мережі (VPN) для безпечного віддаленого доступу.

Література

1. Tanenbaum, A. Computer Networks (5th ed.). / A. Tanenbaum, D. Wetherall. - Pearson Education, 2010. – P. 368-370. http://iips.icci.edu.iq/images/exam/Computer-Networks---A-Tanenbaum---5th-edition.pdf
2. Lehtinen R. Computer Security Basics / R.Lehtinen, D.Russell, G. T. Gantemi Sr. – O'Reilly, 2006. - https://www.oreilly.com/library/view/computer-security-basics/0596006691/
3. Berg, J. Broadcasting on the Short Waves, 1945 to Today / J. Berg, McFarland. - 2013 – P. 46-115.
4. Vinay S. Pai, Kapil Kumar, Karthik Tamilmani, Vinay Sambamurthy, and Alexander E. Mohr. Chainsaw: Eliminating trees from overlay multicast. In *Proc. of the 4th Int. Workshop on Peer-to-Peer Systems*, volume 3640 of *Lecture Notes in Computer Science*. - 2005. – P. 127–140.
5. Johansen H. New Approaches for Security, Privacy and Trust in Complex Environments / H. Johansen, D. Johansen, R. Renesse, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, R. Solms / IFIP International Federation for Information Processing. Springer US –2006. - P. 373–384.
6. Komashinskiy D. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features / D. Komashinskiy, I. Kotenko // 18th Euromicro Conference on Parallel, Distributed and Network-based Processing. – 2010 – 617 p.
7. Мельник, М. О. Створення вдосконаленого плагіна захисту інформації для інтернет-магазину на платформі word press / М. О. Мельник, А. Р. Агаджанян, Я. Г. Маховська // Інформатика та математичні методи в моделюванні. – 2015. – Т. 5, № 1. – С. 65-70.

8. Кобозева, А. А. Общий подход к анализу состояния информационных систем как теоретический базис для стеганоалгоритмов, устойчивых к атаке сжатием / А. А. Кобозева, М. А. Мельник, П. Е. Баранов // Інформатика та мат. методи в моделюванні. – 2014. – Т. 4, № 2. – С. 99-104.
9. Iris localization in biometric personal identification systems developed for mobile devices / K. O. Tryfonova, E. I. Grishikashvili, O. V. Narimanova, A. R. Agadzhanyan // Informatics and mathematical methods in modelling. – 2015. – Vol. 5, N 2. – P. 115-121.
10. Кушниренко, Н. И. Метод криптографической передачи информации на базе эквивалентного класса совершенных двоичных решеток / Н. И. Кушниренко, В. Я. Чечельницкий // Інформатика та математичні методи в моделюванні. - 2014. - Т. 4, № 3. - С. 210-218.
11. Сиропятов, О. А. Сравнительный анализ теоретических подходов моделирования трафика с точки зрения соответствия сетям нового поколения / О. А. Сиропятов, В. Я. Чечельницкий // Інформатика та мат. методи в моделюванні. - 2013. - Т. 4, № 1. - С. 57-67.