2. Алгоритмический кодграббер и диалоговый код. [Електронний ресурс].–Режим доступу https://www.drive2.ru/b/1619320/

Дзензура А. А.,
Криворізький національний університет
Кумченко Ю. О.
к.т.н., доцент, Криворізький національний університет

ЗАХИЩЕНЕ ЛОКАЛЬНЕ МЕРЕЖЕВЕ СЕРЕДОВИЩЕ ДЛЯ ЗБЕРІГАННЯ ФАЙЛІВ НА ОСНОВІ NAS

Розглянуто основні види загроз та засоби захисту локального мережевого середовища на основі NAS. Запропоновано схему побудови захисту сервера та зображено типові методи атак.

Тема захисту інформації, загалом конфіденційних даних, є дуже важливою та актуальною у наш час. Власники інформаційних систем, які не надають належної уваги до захисту, ризикують витоком, знищенням та спотворенням важливої інформації.

Мережеве сховище знаходиться в стані захищеності, якщо забезпечена доступність, конфіденційність та цілісність інформації. Дані, які знаходяться в локальних (LAN), або в глобальній мережах (WAN), постійно піддаються різним видам загроз. Найбільш поширеними видами атак, на локальне мережеве середовище для зберігання файлів на основі Network Attached Storage (NAS), є наступні:

1) прослуховування мережі (Sniffing) – крадіжка або перехоплення даних шляхом захоплення мережевого трафіку за допомогою спеціалізованого ПЗ – Sniffer;
2) атака-вторгнення (Invasion Attack) – перехоплення управління ресурсами мережі;
3) відмова в обслуговуванні (Denial of Service) – атака на обчислювальну систему з метою довести її до відмови;
4) ping-флуд (Ping Flooding) – приведення сервера до відмови шляхом великої кількості запитів;

5) IP-спуфинг (IP Spoofing) – використання чужої IP-адреси з метою обману системи безпеки;

6) шкідливі програми (viruses, worms, troyan horses) та ін.

Є три фундаментальні групи методів захисту мережевого середовища.

Група програмно-технічних засобів до яких входять:

1) аналізатори протоколів;

2) антивірусні програми;

3) міжмережні екрани (брандмауери);

4) криптографічні засоби;

5) системи резервного копіювання.

Група захисту технічних каналів зв'язку до яких входять:

1) використання екранового кабелю;

2) встановлення високочастотних фільтрів;

3) використання екранового обладнання.

Група захисту периметра інформаційного середовища до якого входять:

1) системи охоронної та пожежної сигналізації;

2) системи відео спостереження;

3) системи контроля доступу.

Запропонована схема, яка представлена на рисунку 1, демонструє захист локального мережевого середовища для зберігання файлів на основі NAS від типових методів атак.

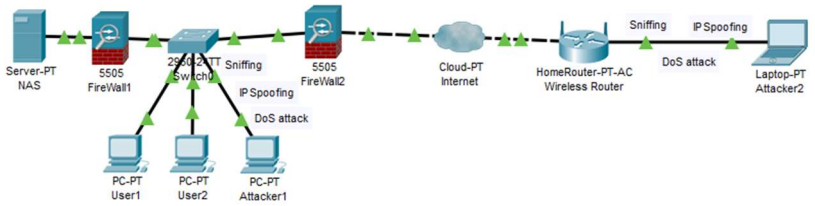

Рис.1 – Схема захисту та нападу на сервер

ВИСНОВКИ

Таким чином захист локального середовища є дуже важливим через велику кількість загроз. Не існує ідеального захисту, тому для

захисту локального мережевого сховища потрібно використовувати комплексні методи захисту.

Мисливець Д. О.,
Криворізький національний університет
Кумченко Ю. О.
к.т.н., доцент, Криворізький національний університет

СИСТЕМА ЗАХИСТУ КОМП'ЮТЕРІВ МЕТОДОМ ФІЛЬТРАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

Розглянуто актуальність використання брандмауеру для користувачів комп'ютерів. Представлено розмежування контент-фільтрів та класифікацію фільтрації.

У зв'язку з розвитком різносторонніх оновлених мережевих технологій збільшується обсяг інформації, яка передається мережею, а також появою нових протоколів передачі даних прикладного рівня, тому все більшої актуальності в наш час набуває метод фільтрації цього трафіку.

Файєрвол, брандмауер чи мережевий екран – це пристрій забезпечення мережевої безпеки, що здійснює моніторинг вхідного та вихідного трафіку, на базі певних, встановлених правил безпеки, приймаючи рішення про дозвіл чи заборону трафіку в мережі [1]. Реалізація відбувається шляхом використання певного програмного, апаратного, або програмно-апаратного забезпечення. Застосовується як спосіб, щоб забезпечити захист комп'ютера від різноманітних мережевих атак, таких як: шпигунські програми, DDoS-атаки тощо; блокування відвідування заражених вірусами або небажаних інтернет-сайтів; виявлення різноманітних шпигунських засобів стеження за активністю користувача.

ПАРАМЕТРИ КОНТЕНТ-ФІЛЬТРІВ

Системи фільтрації мережевого трафіку можна розділити на такі показники:

1. Підзвітність. Оцінює кількість участі населення в політиці фільтрації контенту.