ДОДАТОК А
ПУБЛІКАЦІЯ ЗА ТЕМОЮ РОБОТИ

СЕКЦІЯ 11.
ЕЛЕКТРОНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

СЕКЦІЯ 12.
КОМП'ЮТЕРНА ТА ПРОГРАМНА ІНЖЕНЕРІЯ

Житник Владислав Юрійович, здобувач вищої освіти
факультету інфокомунікацій
Харківський національний університет радіоелектроніки, Україна

Науковий керівник: Штих Інна Анатоліївна, старший викладач
кафедри радіотехнологій інформаційно-комунікаційних систем
Харківський національний університет радіоелектроніки, Україна

НАЛАШТУВАННЯ БЕЗПЕКИ МАРШРУТИЗАТОРІВ CISCO

На противагу звичній для нас життєвій мудрості: «Все, що не заборонено, - дозволено», з позицій захисту маршрутизатора будемо керуватися прямо протилежним постулатом: забороняти все, крім того, що дозволено. Крім цього, гарною ідеєю є заборона того функціоналу, який буде використовуватися рідко, не має сенсу у використанні або призначення якого нам не зовсім зрозуміле. Звісно, останній пункт має бути винятком, оскільки ми завжди можемо ознайомитися з величезним набором документації [1].

Загальний план фундаментального захисту маршрутизатора матиме такий вигляд [1]:

- налаштування аутентифікації та паролів;
- обмеження доступу до маршрутизатора;
- вимкнення зайвих служб і ввімкнення додаткових служб;
- налаштування SNMP;
- налаштування журналювання.

Підміна IP-АДРЕС – одна з критичних проблем протоколу IP версії 4, полягає вона в тому, що найчастіше більшість маршрутизаторів налаштовані на перенаправлення пакетів, виходячи тільки з даних у полі адреси призначення заголовка IP. Звісно, проблема полягає не в самому механізмі маршрутизації, а в тому, що в більшості мереж абсолютно будь-який коректно сформований пакет можна буде вільно перенаправити, якщо маршрутизатор матиме маршрут до адреси призначення, навіть якщо в полі адреси джерела заголовка IP буде вказано нелегітимну адресу. Подібна нелегітимна (фейк) адреса в умовах нормального функціонування мережі зазвичай не може бути вказана як джерело пакета, і найчастіше причиною її появи може стати лише те, що хтось, а точніше, щось не бажає показати, звідки насправді прийшов пакет [1].

Простіше кажучи, причиною появи в мережі подібних пакетів найчастіше є шкідливе програмне забезпечення, чи то хробаки, чи то віруси, чи то спам- або DDoS-боти. Звичайно, приховати їхню діяльність дуже складно, і будь-який більш-менш досвідчений мережний адміністратор за бажання досить швидко виявить їхню мережну активність. Візьмемо, наприклад, процес розсилки спаму. Найчастіше ним займатимуться керовані боти, особливий клас шкідливого програмного забезпечення на кшталт троянів-бекдорів, централізовано керованих із майстер-сервера. Спам-бот, коли отримав команду від господаря через майстер-сервер, у великій кількості розсилає кореспонденцію, відкриваючи безліч tcp-з'єднань на 25-ті порти (SMTP) різних серверів. При цьому в кеші маршрутизатора мережний

адміністратор спостерігає записи [1].

Як відомо, останнім часом атаки на кшталт TCP SYN-flood поступово сходять нанівець, завдяки старанням Microsoft щодо захисту своїх ОС Windows від безконтрольного використання сирих сокетів, що дають змогу конструювати мережні пакети "вручну". Зважаючи на вищеназвані обставини, дедалі більшої популярності набувають атаки на кшталт ICMP/UDP флуд або атаки, спрямовані на відмову в обслуговуванні Web-сервісів шляхом їхнього перевантаження POST/GET-запитами.

Список використаних джерел:

1. Уэнделл Одом. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-105: маршрутизация и коммутация, академическое издание. / акад. изд. : Пер. с англ. - М. : ООО. "И.Д. Вильяме", 2018. – 903 с.