УЯЗВИМОСТИ FIREWALL

Плис А. Д., Черменева И. П.
Научный руководитель: Черменева И. П.
Черноморское высшее военно-морское училище имени П. С. Нахимова, Россия
E-mail: ldebian@mail.ru

Аннотация — Firewall это программа, созданная для защиты сетей. Она осуществляет фильтрацию пакетов и трафика, как внешнего WAN, так и внутреннего LAN.

1. Введение

В наше время существует много способов организовать защиту, но ни один из них не способен найти все угрозы. Поэтому предлагается разработка приложения, которое могло бы существенно сократить количество “хакерских атак”.

2. Основная часть

Firewall уязвимы к таким типам вирусов, как:

— RAT, RMS, BOTNet, MBC, Banner, worm, trojan;

— уязвим к простейшим сканерам типа Nmap netgstat.

Эти недостатки данного программного продукта не могут на 100 % обеспечить защиту компьютерных сетей предприятий, учреждений и организаций, домашних сетей.

Как известно, программный продукт Firewall подразделяется на 5 классификаций:

— управляемые коммутаторы (осуществляющие фильтрацию трафика);

— пакетные фильтры (контроль трафика на сетевом уровне);

— шлюзы сеансового уровня (исключают взаимодействие внешних хостов с узлом в локальной сети);

— посредники прикладного уровня (прикладной уровень прямое взаимодействие двух узлов);

— инспекторы состояния.

Вирусы способны не только отключить Firewall без труда, но и перенастроить или добавить себя в их исключения, и, соответственно, взять под контроль всю сеть предприятия или домашнюю сеть. [1]

Есть и локальные перехватчики трафика, такие как: nmap, Nshark, netlook, Nscam и др. Данные перехватчики способны вычислять открытые, рабочие порты — осуществлять перехват пакетов и их замену.

На рис. 1 изображена таблица сетевого фильтра в действии.

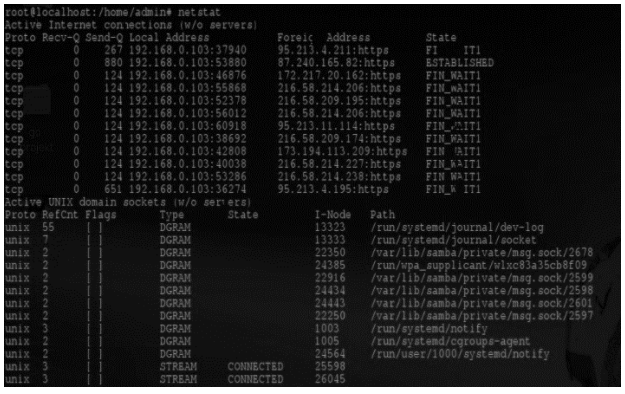

Рис. 1

В целом, сетевые экраны, созданые на операционной систему linux показывают лучшие результаты. Эта операционная система не имеет реестра как у ОС Windows, что позволяет устранить большую часть уязвимостей, создавать сетевые экраны в два раза быстрее и проще. Но большая часть пользователей пользуется Windows. Поэтому, предлагаю модернизировать сетевые экраны, добавив отдельную среду, которая бы не касалась процессов Windows и добавляла в свои исключения только те приложения, которые получили специальный ключ после их проверки. Данная среда сократила бы возможные сетевые угрозы и помогла бы бороться со взломами.

3.Заключение

Данная технология могла бы поднять производительность компьютера минимум на 2 %, увеличить скорость обработки сетевых пакетов. На новой версии ОС Windows 10 было добавлено ядро linux. Данное ядро позволит разработать такую среду и оптимизировать её, а так же даст возможность восстановления повреждённых сигнатур.

4. Список литературы

[1] Лапонина, О. Р. Межсетевое экранирование / О. Р. Лапонина. — САОА, 2002. — 345 с.

FIREWALL VULNERABILITY

Plis A. D., Chermeneva I. P.
Scientific adviser: Chermeneva I. P.
Nahimov Black Sea Higher Naval School, Russia

Abstract — Firewall is the software for defense of networks. The program filter packet and traffic for external WAN, as well as for inner LAN.