АЛГОРИТМИЧЕСКОЕ РЕШЕНИЕ ЗАДАЧИ СИНТЕЗА ПРАВИЛ ДОСТУПА НА ОСНОВЕ ТЕЛЕМЕТРИИ СЕТЕВЫХ ПОТОКОВ

Редькин Ю.В., канд. техн. наук, доцент,

Рябуха А.Г., магистрант,

Пешков А.В., магистрант

ФГБОУ ВО «ГМУ им. адм. Ф.Ф. Ушакова»,

г. Новороссийск, Россия

Аннотация. В работе предложен метод автоматического синтеза правил пакетного фильтра pf на основе анализа потокаNetFlow,получаемого от программного шлюза FreeBSD. Представлен скрипт фильтра, выделяющий устойчивые каналы связности графа локальной вычислительной сети при наличии фонового сканирования портов Nmap. Приведен пример лога nfdump, структура рабочего кода и результаты статистических исследований тестируемого

стенда. Показано, что предлагаемый метод позволяет изолировать узлы локальной сети внутри широковещательного домена и исключает попадание сканирований в разрешающие правила.

Ключевые слова: микросегментация, NetFlow, FreeBSD, списки доступа ACL, сканирование портов.

В настоящее времяосновной подход к защите локальных сетей базируется на концепции «замковой защиты» (Castle-and-Moat), при которой основной комплекс защитных мер концентрируется на внешнем периметре с помощью межсетевых экранов (МЭ), систем обнаружения и предотвращения вторжений (IDPS) и VPN-шлюзов. При этом внутреннее пространство сети, как правило, сегментируется лишь укрупненно – путем выделения нескольких виртуальных локальных сетей (VirtualLo calAreaNetwork , VLAN).

Разбив сеть на подсети тегами 802.1Q, удается защититьее периметр, но при этом остается открытым весь внутренний L2-домен: узлы свободно обращаются по MAC -адресам через общий коммутатор. Таким образом, методы разграничения сетевого доступа, базирующиеся на изоляции широковещательных доменов посредством виртуальных локальных сетей VLAN и статических межсетевых экранов, не предотвращают развитие атак с горизонтальным перемещением нарушителя (lateralmovement) внутри периметра.Как следствие, если на сетевой компьютер попадает вредоноснаяпрограмма, то он сразу начинает опрос соседей по портам 445 (SMB), 135 (RPC) и 3389 (RDP

). Для портовых терминалов и судовых сетей,объединяющих навигационные мостики (IBS), автоматику контроля энергоустановок и терминалы спутниковой связи в общую локальную сеть Ethernet , такое горизонтальное перемещение нарушителя оказывается критичным[6]. Создать жесткие списки доступа (ACL) вручном режиме сетевому инженеру, как правило,не позволяет отсутствие документации на используемыепрограммные продукты, а попытки блокировать порты экспериментальным путем приводят к простоям [1].

...

полный текст во вложении