УДК 004.056

Беляев П.А.

магистрант

Научный руководитель: Макаров И.С., к.т.н

Поволжский государственный университет телекоммуникаций и информатики

СИСТЕМЫ МОНИТОРИНГА И АНАЛИЗА СЕТЕВОГО ТРАФИКА

Аннотация: в научной статье посвящена актуальности проблемы анализа сетевого трафика для защиты от несанкционированного воздействия. Рассмотрены существующие способы решения данной проблемы. Рассмотрены методики обнаружения аномального и злоумышленного поведения пользователей.

Ключевые слова: мониторинг, анализ, трафик, система, сети

Belyaev P.A.

undergraduate

NETWORK TRAFFIC MONITORING AND ANALYSIS SYSTEMS

Abstract: The scientific article is devoted to the relevance of the problem of analyzing network traffic to protect against unauthorized exposure. Suitable solutions to this problem are considered. Methods for detecting detection and malicious user behavior are considered.

Keywords: monitoring, analysis, traffic, system, networks

Из-за активного роста компьютерных сетей появляются новые протоколы передачи данных, а также происходит увеличение потребителей информационных услуг и размеры передаваемого трафика.

Но такой бурный рост приносит кучу проблем. Одной из таковых является серьезные условия для выбора сетевой и серверной аппаратуры,

необходимое для беспрерывного обмена информацией. Вторая проблема заключается в защите данных, перемещающихся по сети.

В качестве решения данных задач применяют мониторинг, а также исследование трафика, которые отлично помогают при возникновении данных проблем. Также нужно понять, что данные перемещаются по сети беспрерывно, соответственно и сбой аппаратуры влечет за собой к огромным финансовым потерям организации. Именно поэтому возникает необходимость в наблюдении за течением сетевого трафика и регулярной проверке на уязвимости в политике безопасности.

Средства для наблюдения и анализа информационных сетей имеют несколько направлений, такие как:

Network Management Systems-системы сбора информации о данных в сети, а также состоянии аппаратуры. Спектр возможностей этих программных средств достаточно обширен. Концепции управления сетью функционируют в автоматизированном порядке, также способны сделать несложные действия на автономном уровне и оставить серьёзный выбор пользователю на базе уже собранной системой информации.

Embedded systems- системы, представленные в виде модулей, которые либо встроены модули связи или операционную систему. Как следует из определения они собирают данные только об оборудовании, на котором оно располагается. Как правило интегрированные модули управления также выполняют роль SNMP-агентов, передавая данные о состоянии устройства в систему управления.

Protocol analyzers-– это программные или аппаратно-программные системы, используемые только для мониторинга и анализа трафика в сетях. Хорошим анализатором считается тот, который может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях - примерно нескольких десятков. Эта группа систем может

устанавливать некоторые логические условия для захвата отдельных пакетов и выполнять полное декодирование пакетов, то есть отображать в удобной для пользователя форме вложенность пакетов протоколов разных уровней с расшифровкой содержания каждого полей пакета.

Внедрение подобных систем для защиты информации является необходимостью для всех серьезных сетевых инфраструктур, так как существуют программы, которые постоянно выискивают уязвимости в любом оборудовании, подключенном к глобальной сети.

Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS)) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть.

Система предотвращения вторжений (СПВ) (англ. Intrusion Prevention System (IPS)) – программное или аппаратное средство, осуществляющее мониторинг сети или системы в реальном времени с целью выявления, предотвращения или блокировки вредоносной активности.

Использованные источники:

1. Cecil Alisha. A Summary of Network Traffic Monitoring and Analysis Techniques [Электронный ресурс] : статья / Alisha Cecil // сайт Вашингтонского университета в Сент-Луисе. – Режим доступа: http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html
2. IDS/IPS — Системы обнаружения и предотвращения вторжений [Электронный ресурс]: статья. Режим доступа: http://netconfig.ru/server/ids-ips/.
3. IDS/IPS - системы обнаружения и предотвращения вторжений и хакерских атак [Электронный ресурс]: статья // сайт компании «АльтЭль». – Режим доступа: http://www.altell.ru/solutions/by_technologies/ids/.
4. WinPcap Documentation [Электронный ресурс]: документация. – Режим доступа: http://www.winpcap.org/docs/docs_412/html/main.html