Газпром Нефть

Система обнаружения внешних каналов связи с сетью Интернет

Контекст / описание проблемы:

Для многих крупных территориально распределенных компаний, заботящихся о своей информационной безопасности, актуальной является проблема обнаружения и нейтрализации несанкционированных внешних каналов связи с сетью Интернет. Ведь ни для кого не секрет, что 80% атак происходит изнутри компании и важной задачей злоумышленника является наличие не контролируемых каналов связи с сетью интернет. Организация подобных не контролируемых каналов связи с сетью интернет возможно через сторонние (некорпоративные) шлюзы доступа к интернету (модемы, смартфоны и т. д.).
Задача данного кейса поиск не санкционированных каналов связи с сетью интернет, организованные внутренними нарушителями через сторонние (некорпоративные) шлюзы доступа в сеть интернет (модемы, смартфоны и т. д.).

Задача:

Разработать алгоритм (блок-схему), программный модуль и архитектуру информационной системы (далее Система) обеспечивающей поиск на корпоративных хостах, подключенных к корпоративной сети передачи данных, не санкционированных каналов связи с сетью интернет.

В работе учитывать следующие моменты:

- доступ корпоративных хостов в сеть Интернет организован через корпоративные прокси-сервера;
- на сетевом оборудовании отключена маршрутизация и преобразование адресов (NAT) между Интернетом и внутренними ("серыми") IP-адресами сети предприятия;
- необходимо предусмотреть выгрузку информации по хостам и учетным записям из AD, с их последующим анализом;
- необходимо проработать механизм доставки и периодического запуска разработанного программного модуля на хостах;
- разрабатываемый модуль должен осуществлять поиск максимального количества используемых несанкционированных прокси, в том числе прописанных в расширениях браузера, а также других несанкционированных каналов;
- предусмотреть функционал по анализу полученных результатов;
- предусмотреть меры по защите информации передаваемой разработанным программным модулем и защите разработанной Системы;
- пользователями Системы являются сотрудники подразделений по защите информации.

Требования к решению:

Для оценки предложенных решений необходимо предоставить:

1. Алгоритм (блок-схему) работы программного модуля, обеспечивающего выявление не санкционированных каналов связи с сетью интернет.
2. Архитектуру Системы обеспечивающей функционирование программного модуля.
3. Программный модуль обеспечивающей поиск на корпоративных хостах, подключенных к корпоративной сети передачи данных, не санкционированных каналов связи с сетью интернет.

Технические требования к решению:

Архитектуру Системы необходимо предоставить:

- в виде схемы структурной, на которой должны быть отражены все сервера, АРМ и сетевое оборудование необходимое для обеспечения функционирования Системы. На данной схеме также отразить элементы корпоративной инфраструктуры с которыми осуществляет взаимодействие Система (Сервера СУБД, сервера AD, активное сетевое оборудование, АРМ и т.д.).
- в виде текстового описания информационных потоков Системы.

Программный модуль должен выводить имя хоста, IP адрес, сетевой интерфейс, временную метку и учетную запись имеющую не санкционированный канал связи с сетью интернет.

Критерии оценки:

- Критерий: Уровень проработанности алгоритма (блок-схемы) работы программного модуля
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Критерий: Полнота архитектуры системы
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Критерий: Наличие текстового описания информационных потоков системы
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Наличие отлаженного, работающего программного модуля
  Шкала оценки: максимальный балл - 5, минимальный балл - 1

Возможно получение дополнительных 5 баллов за оригинальность и новизну предлагаемых технических решений задачи.