ОРДЕНА ЛЕНИНА
ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
им. М.В.Келдыша
Российской академии наук

А.В.Ермаков

Использование сетевого сканера для повышения защищенности корпоративной информационно-вычислительной сети

Москва, 2001

УДК 519.68

А.В.Ермаков

Использование сетевого сканера для повышения защищенности корпоративной информационно-вычислительной сети.

В работе дается подробное описание функциональных возможностей и технологии использования сетевого сканера, предназначенного для обнаружения уязвимостей в системе защиты различных сетевых ресурсов.

Исследования системы защиты корпоративной информацинно-вычислительной сети, проведенные в Институте прикладной математики им.М.В.Келдыша РАН, позволили, прежде всего, оценить защищенность сети в целом, найти слабые места, разработать методику повышения надежности и безопасности сетевых ресурсов.

Ключевые слова и фразы: сетевой сканер, безопасность, компьютерная сеть.

A.V.Ermakov

Using network scanner for increasing security of the corporate information network.

The detailed description of network scanner functionalities and technologies of detecting vulnerability in a system of various network resources protection using network scanner is given.

Researches of the system of corporate information computer network protection, carried out at the Keldysh Institute of Applied mathematics of the Russian Academy of Science, first of all, have allowed to estimate network security as a whole, to find weak spots, and to develop a technique of increasing network resources reliability and security.

Key words and phrases: network scanner, security, computer network.

Введение

С ростом компьютерных сетей и развитием Internet-технологий становится все более актуальной проблема защиты информационно-вычислительных ресурсов. Вопрос ставится о защите не только информации, но и информационной системы в целом.

Проблема защиты информационных ресурсов – это проблема всего человечества. Для регистрации и поиска путей защиты обнаруженных уязвимостей (vulnerability) и дефектов в операционных системах, сетевых протоколах и сервисах совместными усилиями корпораций, работающих в области информационных технологий, создан комитет CVE (Common Vulnerabilities and Exposures). На его Web-сайте http://CVE.mitre.org/ публикуется различная информация по обсуждаемой проблеме.

Практически все корпоративные информационные системы уязвимы в той или иной мере для внешних и внутренних атак. В большинстве случаев пользователи даже не подозревают, что в их компьютере или сегменте компьютерной сети содержатся уязвимости, позволяющие недоброжелателю несанкционированно проникать в информационную систему. Реальное представление о недостатках защиты пользователи получают как правило уже после совершения взломов, проникновения вирусов или вывода из строя различных сетевых узлов.

Для построения системы защиты необходимо определить сетевые ресурсы, которые могут подвергаться атакам со стороны злоумышленников. Затем следует проанализировать текущее состояние этих ресурсов с точки зрения их защищенности. В случае обнаружения уязвимостей необходимо срочно принять соответствующие меры по их защите.

Данная работа посвящена вопросам обнаружения недостатков в системе защиты различных сетевых ресурсов – как первому шагу повышения безопасности корпоративной информационно-вычислительной сети.

1. Сканеры защищенности сети

Для обнаружения уязвимостей ресурсов информационной сети используют специализированные программные продукты, называемые сканерами защищенности (security scanner).

В мире существует большое количество сканеров защищенности, которые можно подразделить на два типа: диспетчер/агент и сетевой сканер.

Системы с архитектурой диспетчер/агент осуществляют проверку защищенности сетевых ресурсов с центральной консоли, получая информацию от программных агентов, установленных на конечных системах. К системам такого типа относятся Enterprise Security Manager от компании Axent Technologies.

Принцип работы сетевых сканеров заключается в следующем.

1. Компьютер с установленным на нем сканером подключается к Интернет.
2. В заданном диапазоне IP-адресов производится поиск доступных сетевых ресурсов, идентификация сетевых сервисов и анализ их уязвимости.
3. По результатам сканирования автоматически готовится отчет о состоянии защищенности каждого сетевого ресурса, обнаруженных недостатках в системе защиты и оценке опасности, с точки зрения использования этих недостатков для проникновения в систему.

Таким образом, сканеры позволяют анализировать работу всех сетевых устройств заданного сегмента сети без вхождения с ними в непосредственный контакт.

Если в базу данных сканера защищенности заложена информация о средствах защиты обнаруженных уязвимых мест, то в отчете появятся и рекомендации по этому поводу.

Получив такого рода отчет, администратор сетевого ресурса может через Интернет попытаться найти необходимые средства защиты или обратиться к специалистам. И делать это нужно незамедлительно, так как точно также проанализировать доступность сетевых ресурсов может и злоумышленник. А затем определить, через какую «дыру» и как можно пролезть в систему.

2. Сканер защищенности Shadow Security Scanner

Сканер защищенности Shadow Security Scanner (SSS) является достаточно мощным и надежным средством для обнаружения недостатков в системе защиты сетевых узлов (персональных компьютеров, рабочих станций, серверов).

Для поиска уязвимостей в сканер встроены как стандартные средства тестирования сети, так и специализированные, имитирующие действия злоумышленника по проникновению в компьютерные системы, подключенные к сети. Гибкая модульная архитектура сканера SSS позволяет постоянно перестраивать его возможности, добавляя новые модули, эмулирующие новые варианты компьютерных атак.

Процесс сканирования можно изобразить в виде пошаговой процедуры, представленной на рис.1, семь этапов которой однозначно соответствуют функциональным частям сетевого сканера:

1. Задание параметров сеанса сканирования;
2. Автоматическое обнаружение сетевых ресурсов;
3. Сбор данных;
4. Анализ данных;
5. Определение уязвимостей;
6. Представление результатов сканирования;
7. Автоматическая подготовка отчета.

Рис.1. Схема проведения сканирования сегмента сети.

2.1. Настройка сеанса сканирования

Установка сканера не составляет большого труда, поэтому не будем подробно останавливаться на этом вопросе.

Сканер предоставляет дружественный интерфейс и удобное меню, основные функции которого вынесены в виде «иконок», как показано на рис.2.

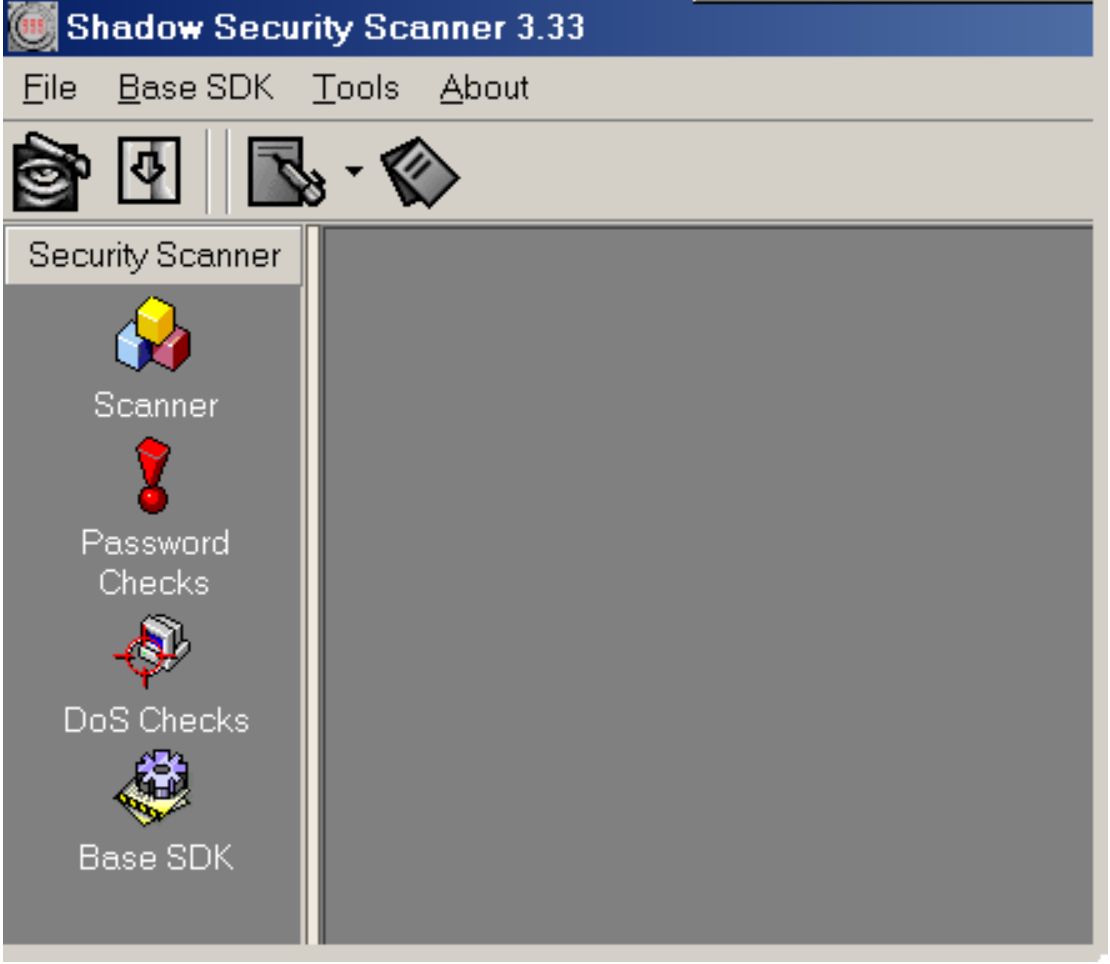


Рис.2. Главное меню сканера.

В следующих разделах мы подробно рассмотрим возможности этого сетевого сканера, основываясь на поэтапной процедуре сканирования, показанной на рис.1, а в данном разделе отметим некоторые ключевые моменты, связанные с заданием и настройкой базовых параметров сканирования:

- задание диапазона IP-адресов (рис.3);
- задание сканируемых портов (рис.4);
- задание анализируемых сетевых служб (рис.5).

Задание области сканирования

Задаваемый диапазон IP-адресов может быть непрерывным, разрывным, из него могут быть удалены какие-то отдельные узлы – эти параметры задаются пользователем в каждом конкретном сеансе сканирования.

Задавая область сканирования, пользователь может использовать следующие функции:

- добавить узел (Add Host);
- добавить диапазон (Add IP Zone);
- исключить узел (Delete Host).

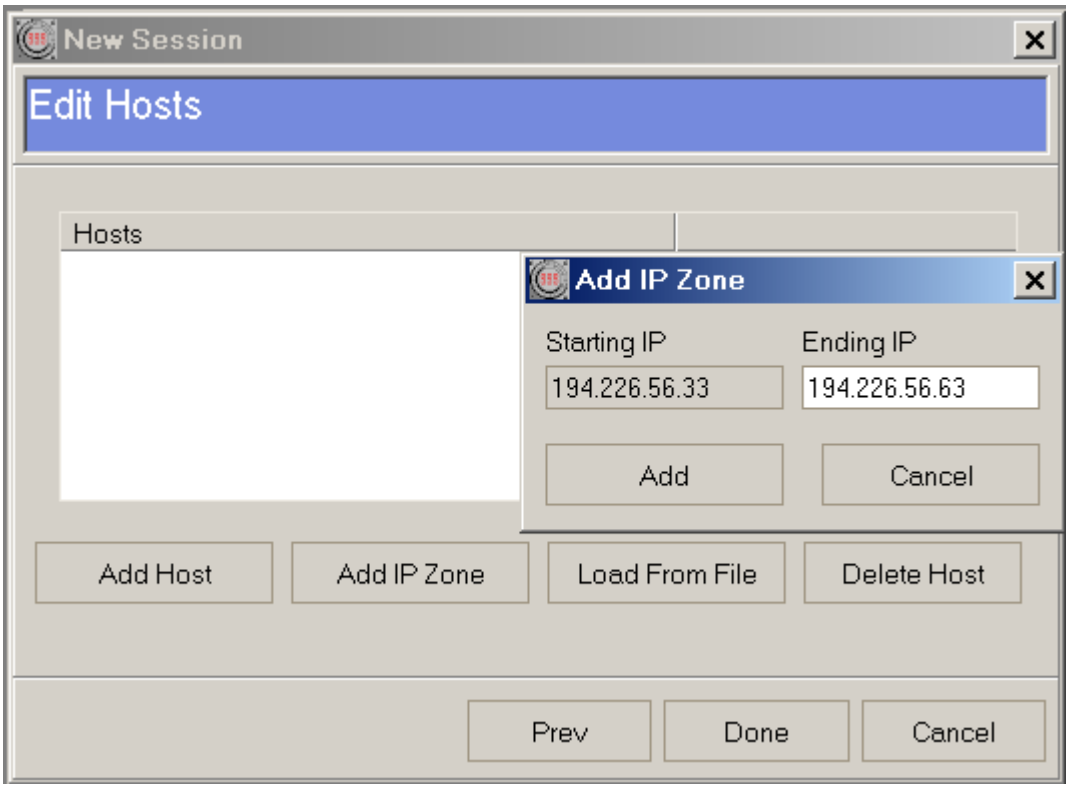


Рис.3. Задание диапазона сканирования.

Задание сканируемых портов

Порты компьютера или любого другого активного сетевого устройства служат для организации взаимодействия по какому-либо сетевому протоколу. Их назначение и способы использования стандартизованы и для любой операционной системы абсолютно одинаковы. Например:

21 порт – FTP (File Transfer Protocol);

22 порт – SSH (Secure Shell Remote Login Protocol);

23 порт – TELNET;

и т.д.

Если порт открыт, то по соответствующему протоколу приложение может связаться с одним или несколькими другими узлами в сети. Но это и есть источник опасности, так как связаться с некоторым узлом в сети можно не только с целью информационного обмена, но и с «вредными помыслами».

У серверных систем (типа Windows NT или UNIX) обычно открыто значительное число портов – это связано с предоставляемыми этими системами сервисами и это является источником повышенной опасности. При правильной настройке сервисных служб опасность снижается, но не исключается вовсе. Злоумышленник, как правило, проникнув в систему, первым

делом изменяет настройки, облегчая себе повторное проникновение и создавая больший комфорт в работе (например, включая закрытые протоколы и выключенные службы).

Поэтому для минимизации опасности любому администратору сервера необходимо оставлять минимальное количество открытых портов и постоянно следить за корректностью параметров настройки соответствующих служб (здесь сетевой сканер подходит идеально, но об этом далее).

У клиентских систем (типа Windows 95/98) обычно все порты закрыты. Они открываются при активизации какого-либо сетевого приложения (при считывании или отправке электронной почты, пересылке файлов и т.п.) и закрываются автоматически при его завершении. Ввиду незначительной продолжительности таких операций, угроза проникновения считается незначительной (если только в самом считываемом почтовом послании или скачиваемом файле не содержится пакостей).

Опасность значительно возрастает, когда клиентские рабочие станции объединяют по протоколу NetBIOS (139 порт – NetBIOS Service Session) в локальную сеть с целью использования общих дисковых ресурсов, принтеров, сканеров и т.д. В этом случае каждый участник этого локального объединения должен представлять себе в общем виде те неприятности, которые могут случиться с его системой по вине соседей и, наоборот, с системами соседей по его вине.

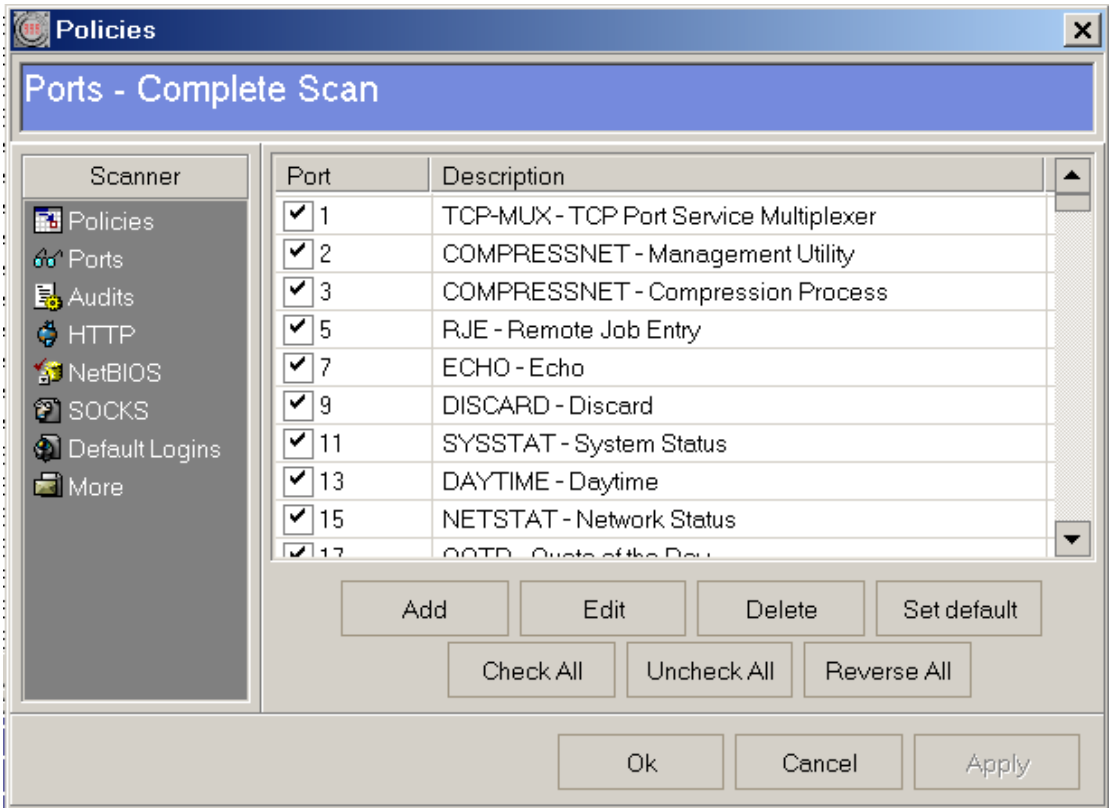


Рис.4. Задание сканируемых портов.

В параметрах настройки сеанса сканирования можно указать все порты (с 1-ого порта по 65301) или выборочно включать/выключать отдельные порты в зависимости от проводимого исследования.

Сетевые сервисы

Как уже отмечалось, наиболее уязвимыми с точки зрения проникновения в систему являются серверные службы. В зависимости от количества включенных серверных служб и качества их настройки эта опасность может возрастать или убывать.

Кроме того, установка дополнительных программных продуктов может изменить какие-то настройки сетевых сервисов, открыть ранее закрытые порты.

Сканер защищенности помогает администратору сервера, во-первых, изначально проверить защищенность системы в целом и, во-вторых, в последующем отслеживать состояние системы защиты. Дело в том, что любой злоумышленник, единожды проникнув в систему, первым делом изменяет параметры настройки для того, чтобы в последующем облегчить себе

проникновение в систему и обеспечить более комфортный режим работы. Эти изменения администратор может обнаружить, воспользовавшись сканером, еще до того, как действия злоумышленника принесут непоправимый вред.

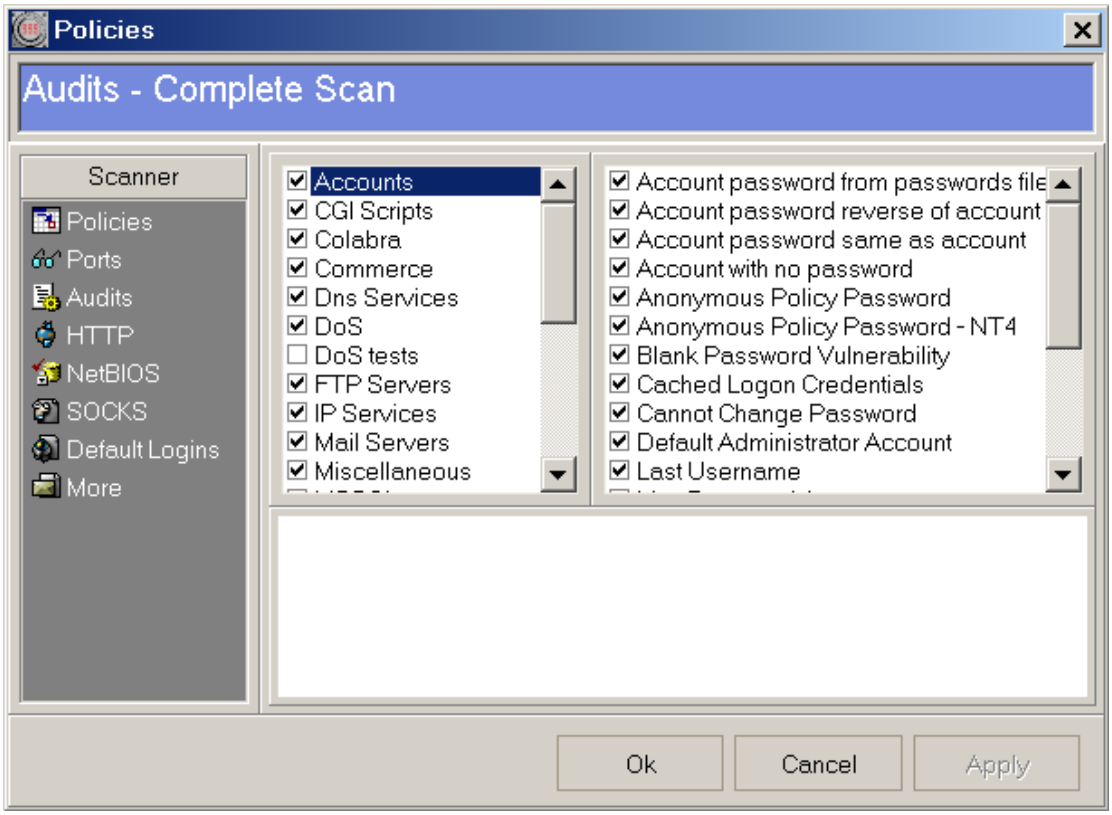


Рис.5. Задание сканируемых сетевых служб.

При настройке параметров сеанса сканирования пользователь может включить все известные сетевые службы или провести выборочное сканирование. Необходимо помнить, что сетевые технологии развиваются стремительно, и появление какого-то нового сервиса может быть не предусмотрено текущей версией сетевого сканера. Помочь в этом случае может только регулярное обновление версии сканера.

Заданием сканируемых сетевых служб заканчивается настройка параметров сеанса сканирования, и затем следует собственно процедура сканирования заданного сегмента сети и анализа собранных результатов (этапы II-VII процедуры, представленной на рис.1).

2.2. Сканирование сетевых ресурсов

Сканирование сетевых ресурсов, автоматическое обнаружение узлов и услуг (рис.6) позволяет собирать информацию о всех сетевых устройствах, находящихся в исследуемой сети, таких как WWW и почтовые сервера, межсетевые экраны, а также маршрутизаторы, сервера удаленного доступа и т.д. Эта функция позволяет пользователям составить полную картину работающих в сети активных устройств и активизированных сетевых услуг путем опроса сетевых устройств по протоколам TCP/IP, SNMP, SMTP и др.

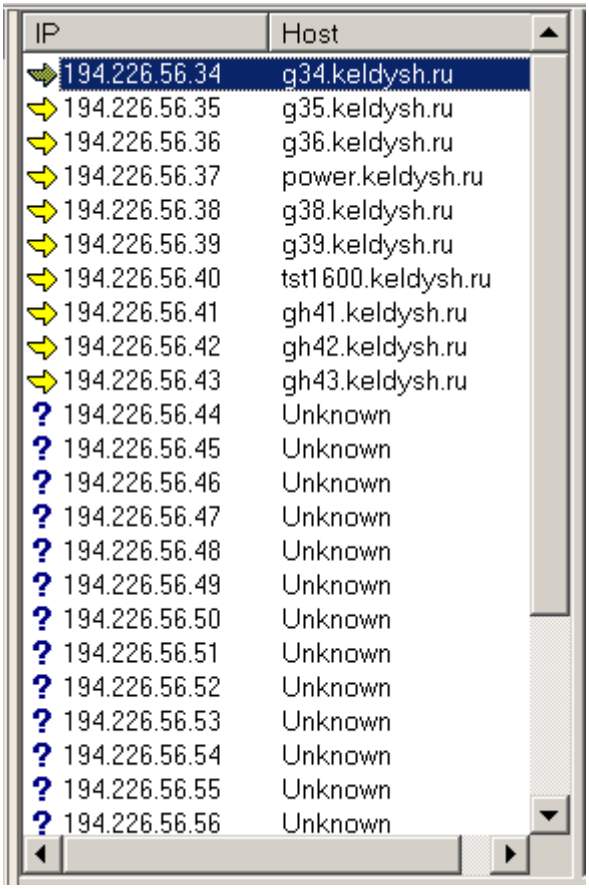


Рис.6. Автоматическое обнаружение сетевых узлов.

Сканер выполняет проверку всех IP-адресов и портов из заданного диапазона и таким образом строит карту сегмента сети.

2.3. Сканирование портов, сбор данных

По созданной карте сегмента сети сканер начинает сбор данных по всем сетевым ресурсам.

Для каждого IP-адреса сканер через службу доменных имен определяет сетевое логическое имя.

Используя процедуру сканирования портов, он определяет активные порты каждого сетевого узла. Как уже отмечалось, в процессе конфигурирования и настройки сетевого сканера можно задать некоторые специальные правила, по которым будет происходить процедура сканирования (например, выборочное сканирования заданных портов или сканирование потенциально наиболее опасных). Естественно, подобное исследование сегмента сети значительно увеличит сетевой трафик. Поэтому, рекомендуется проводить такие исследования в «нерабочее» время.

2.4. Анализ правил

На третьем этапе сканер анализирует собранную информацию с целью определения базовых параметров (типа операционной системы, включенных сетевых сервисов и т.п.) и потенциально возможных недочетов, обычно присутствующих в настройках ОС и сетевых служб, а именно:

- уже обнаруженные «дыры» в Windows NT и UNIX-системах;
- проблемы с настройкой широко используемых сервисов типа telnet, FTP, HTTP - тривиальные пароли и пр.;
- недостатки в настройки специализированных служб типа firewall;
- проблемы в настройке системы электронной почты.

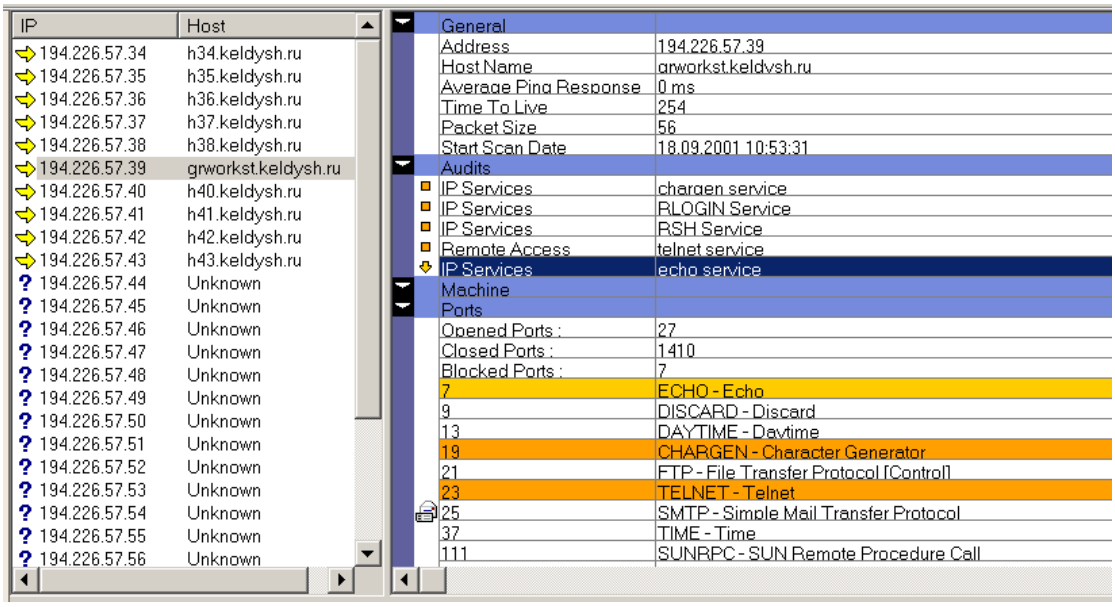


Рис.7. Анализ потенциально опасных мест.

Сведения о вышеуказанных потенциальных ошибках и недочетах в настройке программного обеспечения заложены в базу данных сканера в виде правил, которые система пытается применить для каждого конкретного узла из заданного диапазона.

Эта процедура является «ненавязчивой» – сканер просто перебирает различные варианты уязвимости и отмечает цветом степень их потенциальной опасности (чем краснее – тем опасней).

2.5. Определение уязвимостей

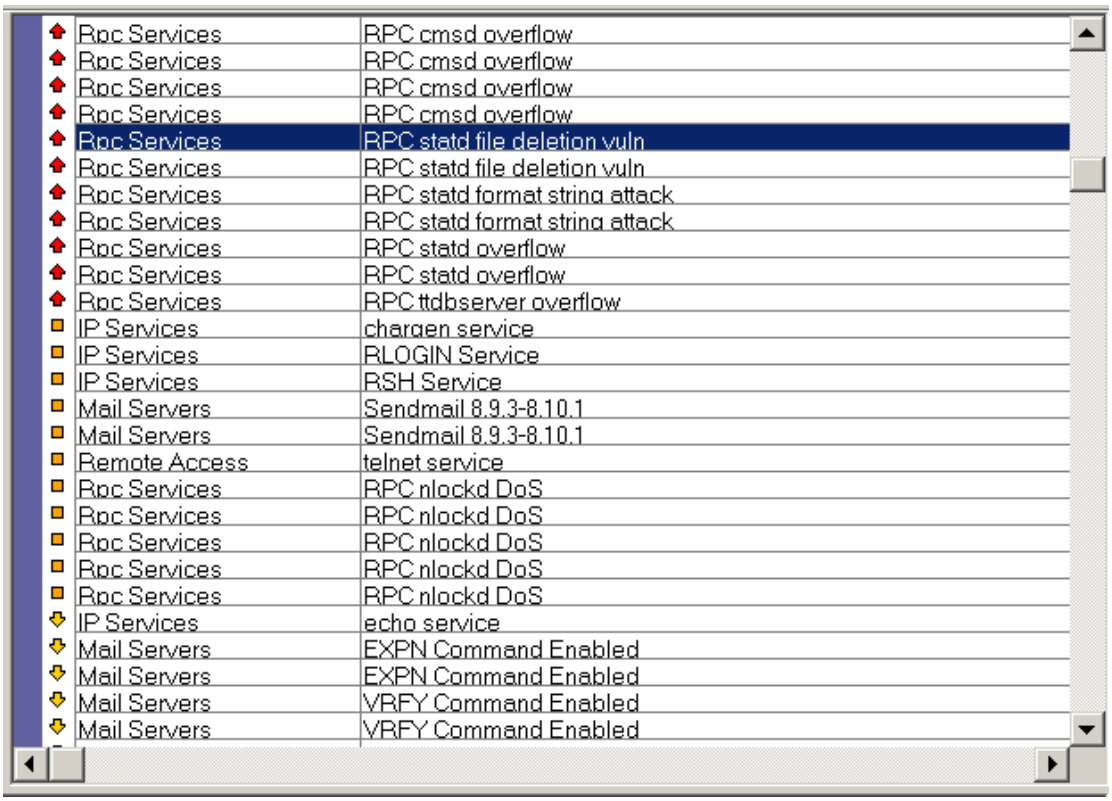
Используя подобранные варианты потенциальных недостатков в системе защиты, сканер пытается проверить, присутствуют ли эти недостатки в каждом из анализируемых узлов. Например, для служб, использующих идентификатор пользователя и пароль для доступа к ресурсам, сканер пытается подобрать пароль.

Этот этап исследования является активным, он предполагает достаточно большое количество запросов, посылаемых по сети к каждому исследуемому узлу (например, при подборе пароля используется база из нескольких тысяч типичных вариантов и плюс генератор паролей), но никаких деструктивных действий сканер не производит.

2.6. Представление результатов сканирования

Результаты сканирования каждого узла сети представляются в виде таблицы, состоящей из четырех разделов:

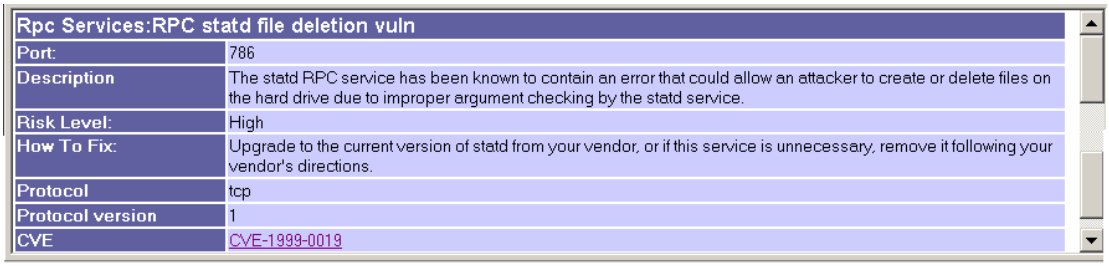
- общие сведения;
- обнаруженные уязвимости;
- операционная система;
- список портов и соответствующих им функций.



Rpc Services	RPC cmsd overflow
Rpc Services	RPC cmsd overflow
Rpc Services	RPC cmsd overflow
Rpc Services	RPC cmsd overflow
Rpc Services	RPC statd file deletion vuln
Rpc Services	RPC statd file deletion vuln
Rpc Services	RPC statd format string attack
Rpc Services	RPC statd format string attack
Rpc Services	RPC statd overflow
Rpc Services	RPC statd overflow
Rpc Services	RPC ttdbserver overflow
IP Services	chargen service
IP Services	RLOGIN Service
IP Services	RSH Service
Mail Servers	Sendmail 8.9.3-8.10.1
Mail Servers	Sendmail 8.9.3-8.10.1
Remote Access	telnet service
Rpc Services	RPC nlockd DoS
Rpc Services	RPC nlockd DoS
Rpc Services	RPC nlockd DoS
Rpc Services	RPC nlockd DoS
Rpc Services	RPC nlockd DoS
IP Services	echo service
Mail Servers	EXPN Command Enabled
Mail Servers	EXPN Command Enabled
Mail Servers	VRFY Command Enabled
Mail Servers	VRFY Command Enabled

Рис.8. Список уязвимых сетевых служб одного из узлов сети.

Как уже отмечалось, сканер обладает удобным дружественным интерфейсом. Выбрав одну из строк списка (рис.7), можно получить краткое описание проблемы (рис.8).



Rpc Services:RPC statd file deletion vuln	
Port:	786
Description	The statd RPC service has been known to contain an error that could allow an attacker to create or delete files on the hard drive due to improper argument checking by the statd service.
Risk Level:	High
How To Fix:	Upgrade to the current version of statd from your vendor, or if this service is unnecessary, remove it following your vendor's directions.
Protocol	tcp
Protocol version	1
CVE	CVE-1999-0019

Рис.9. Описание обнаруженной уязвимости сервиса.

Последняя строка описания обнаруженной проблемы содержит http ссылку на сайт CVE (Common Vulnerabilities and Exposures), где содержится исчерпывающее описание обнаруженной уязвимости системы защиты и рекомендации по ее устранению.

Следующая важная информация, представляемая по результатам сканирования, – список открытых портов и степень их опасности для системы в целом (рис.10).

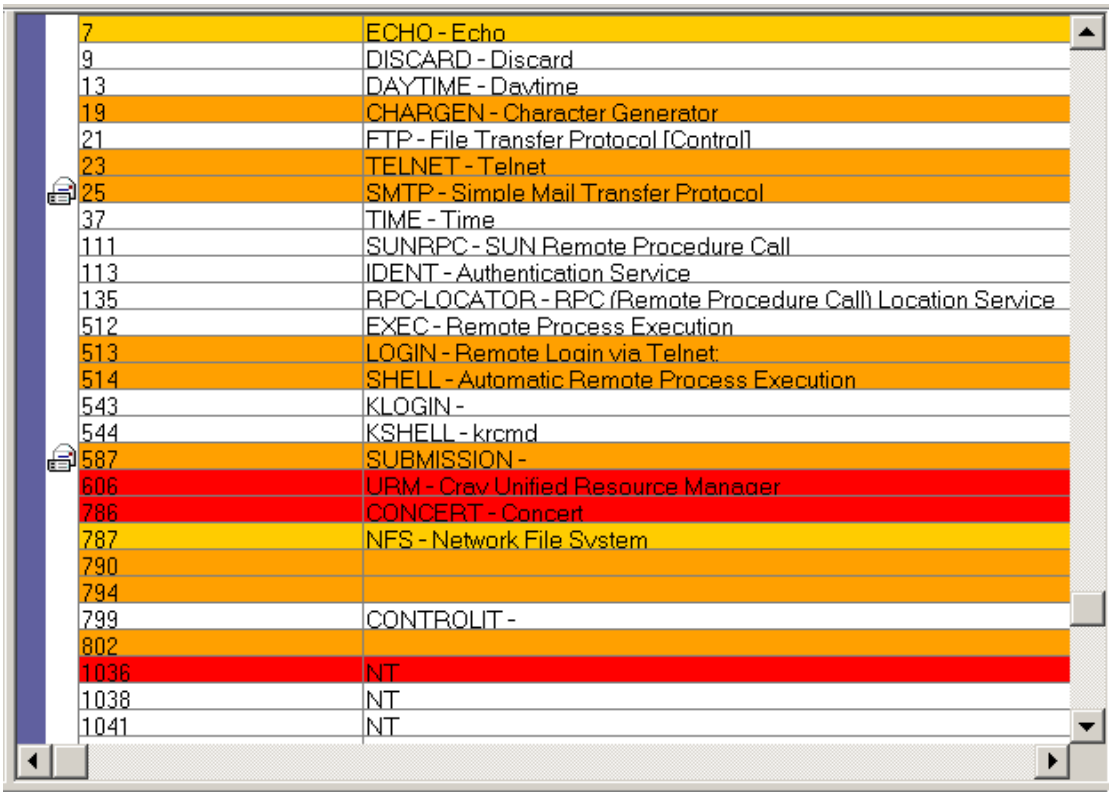


Рис.10. Список открытых портов одного из узлов сети.

На представленном рисунке цветом очень наглядно выделены наиболее уязвимые порты.

2.7. Автоматическая подготовка отчета

Отчет содержит подробные результаты выполненного исследования уязвимости сегмента сети.

Отчет подразделяется на несколько частей.

Первая часть содержит общее описание выполненного исследования, некоторые статистические показатели: число

сетевых узлов, число обнаруженных недостатков в системе защиты, наиболее уязвимые узлы, неудачно настроенные сетевые службы и протоколы.

Вторая часть отчета – результаты сканирования узла сети. В общем-то, в отчете собрана та же информация, которая была рассмотрена в разделе 2.6, но представлена она не в виде одного из окон экранного интерфейса сетевого сканера, а собрана в html-файле, который можно передать для анализа администратору и специалисту по безопасности, или же выложить на Интернет-сайте.

Заключение

В заключение отметим основные результаты проведенного исследования.

Использование сетевого сканера (конкретно SSS или же какого-либо другого) позволяет:

1. наглядно показать администраторам рабочих групп или отдельных серверов недостатки в их системе защиты, помочь в их устранении;
2. вооружить администратора сети мощным инструментом, повышающим безопасность сети за счет ликвидации отдельных уязвимых мест или проведения дополнительных мер по защите сети.
3. Разработать методику, ограничивающую использование в сети высокоопасных сетевых служб и технологий взаимодействия.

Наконец, последний и, может быть, самый важный результат. И без SSS мы, конечно, понимали, что у нас много недостатков в системе защиты серверов, но что их так много, что настолько серьезны эти недочеты – это явилось для нас весьма неприятной неожиданностью.

Оглавление