Вся сеть как на ладони

Фленов Михаил http://www.vr-online.ru

Любой хакер или админ должен знать структуру сети, в которой он находится. Чем больше информации тебе доступно, тем проще будет получить доступ к определенному ресурсу или защитить/взломать его. Хакер должен знать структуру, чтобы увидеть все возможные пути подступа к жертве и возможные варианты обхода через доверяемые машины в сети.

Администам надо знать не только структуру сети, но и доступность различных сетевых и ресурсов. Некоторые лентяи бросают это дело на самотек и когда какой-то сегмент сети вылетает, то только тогда они узнают о проблеме и начинают судорожно пинговать все подряд для выяснения причины. Это глупо и не эффективно, потому что админ теряет информацию о том, когда произошел сбой, а это иногда является самым важным.

Юзеры могут заметить сбой в сети не сразу, а когда заметят, то не сразу сообщат админу о происшедшем. Именно поэтому админ должен сам следить за своими владениями, и не надеяться на дядю Васю.

Постоянно пинговать всю сеть вручную дело не благодарное, утомительное и просто глупое, поэтому настоящие перцы автоматизируют эти задачи. Я тут нарыл в своем архиве несколько прог для облегчения наблюдения за сеткой и сегодня расскажу тебе про них. Все проги мы рассматривать не будем, потому что автоматическое сканирование достаточно сложный процесс и в большинстве программ это реализовано просто ужасно, и включать их в обзор будет просто глупо. Я взял две лучшие тулзы и расскажу тебе только о них.

NetCrunch

Где слить: http://www.adremsoft.com/index.php

Вес: 22 метра

Это наверно самая красивая прога, с которой мне приходилось работать. Ее мне посоветовал M.J.Ash и я не пожалел, Что скачал ее. Это настолько удобная софтвина, что я проигрался с ней целых два дня, чтобы ощутить все ее прелести и рассказать тебе о самом интересном.

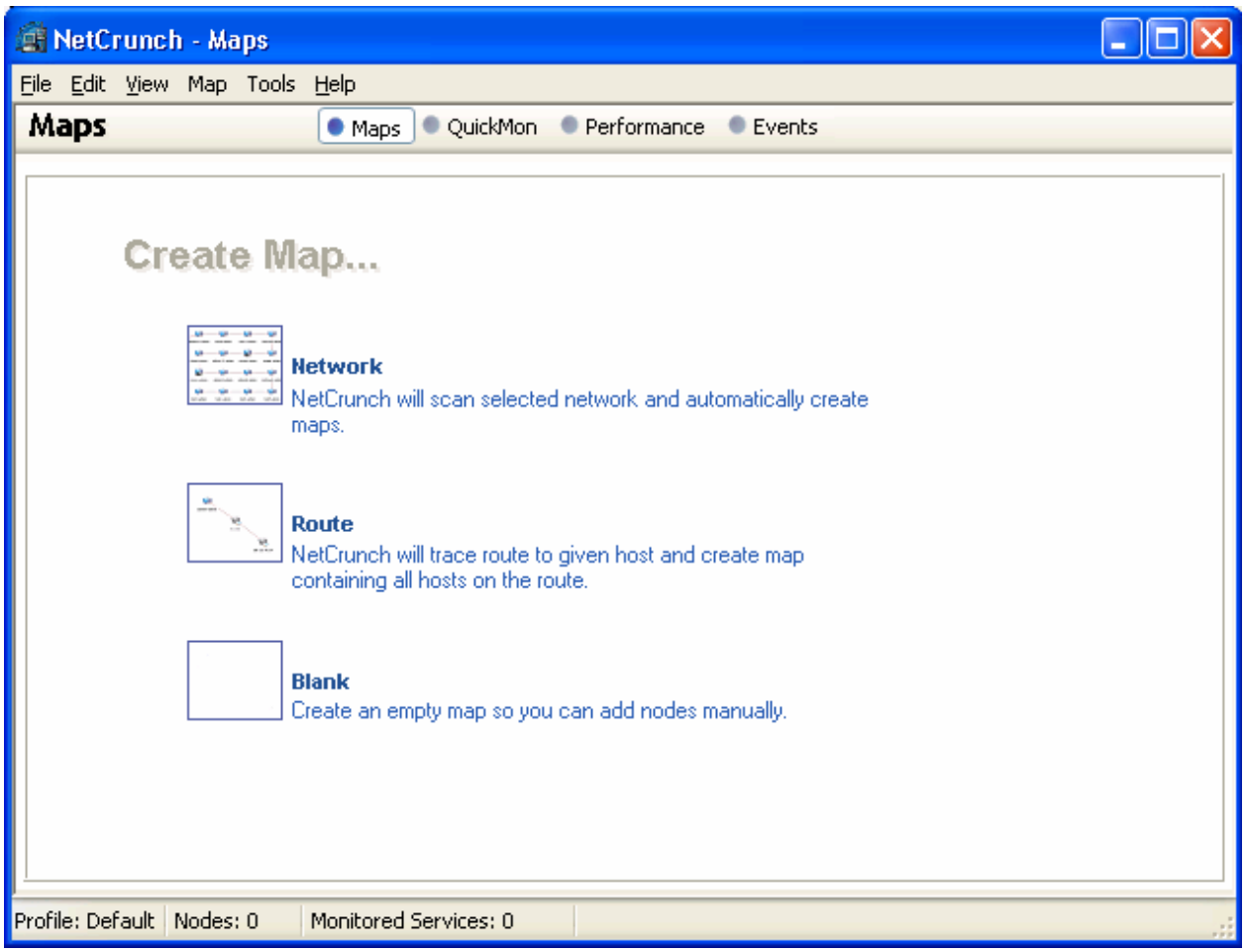
В главном окне программы ты можешь наблюдать три пункта:

Network – автоматическое сканирование сети;

Route – сканирование маршрутизатора;

Blank – создать пустой проект и вручную расставить сетевые ресурсы.

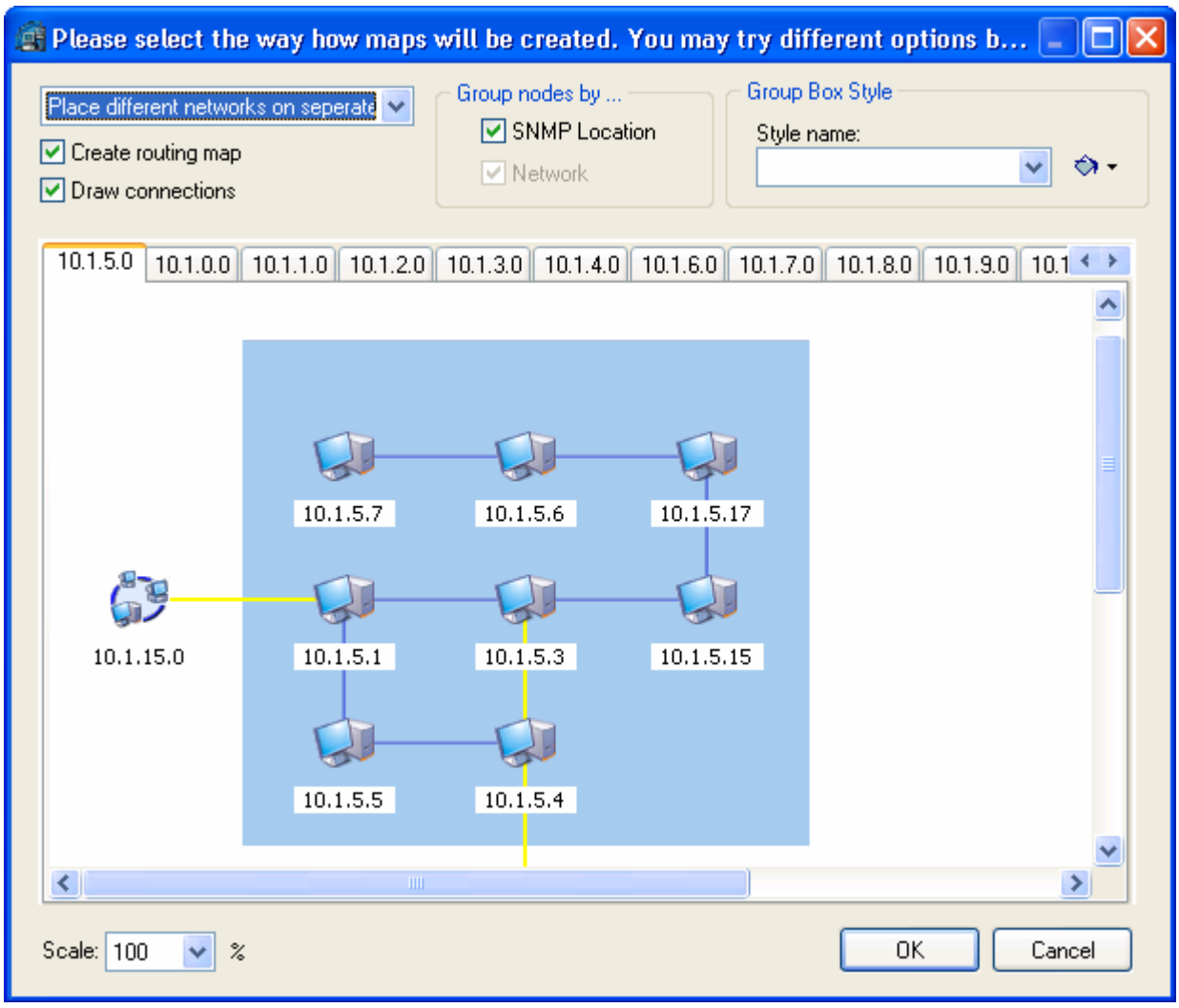
Программа может просканировать только указанную сети или все, включая подсети. Когда она находит какие-то ресурсы, то появляется окно с предложением добавить в мониторинг только первый найденный адрес (нужно для мониторинга доступности сети), выбрать нужные адреса вручную или добавить все.

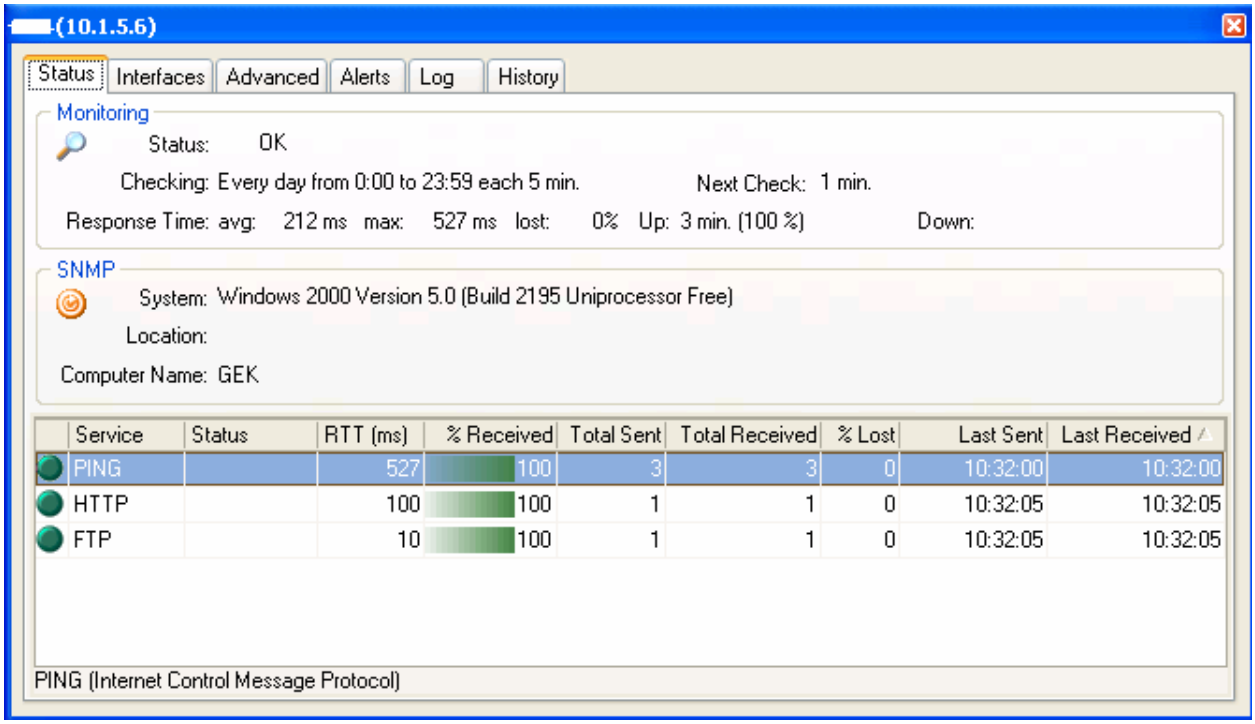


На рисунке 2 показан результат сканирования моей сети. В центре ты можешь видеть окно с закладками. Каждая закладка – это отдельная сеть, а внутри нее показаны компьютеры сети. Если изображение компьютера цветное, то компьютер доступен, если серое, то компьютер не доступен. Таким образом, ты можешь визуально наблюдать за доступностью любого компьютера.

Самая последняя закладка Routing Map показывает карту маршрутизации. Если у тебя сложная сеть, то, глядя на эту карту можно не на шутку испугаться.

Нажми OK, чтобы сохранить структуру сети. Теперь у тебя главное окно изменилось и сверху окна ты можешь выбирать сети, а в центре показана найденная структура. Если щелкнуть правой кнопкой по какому-нибудь компьютеру и выбрать пункт меню Status, то ты увидишь окно, в котором можно увидеть состояние компьютера и его сервисов. Если на нем есть такие сервисы как HTTP или FTP, то прога автоматически проверяет их доступность.





На закладке History ты можешь просмотреть историю доступности ресурса и таким образом узнать, когда он был в сети, а когда происходили какие-то сбои.

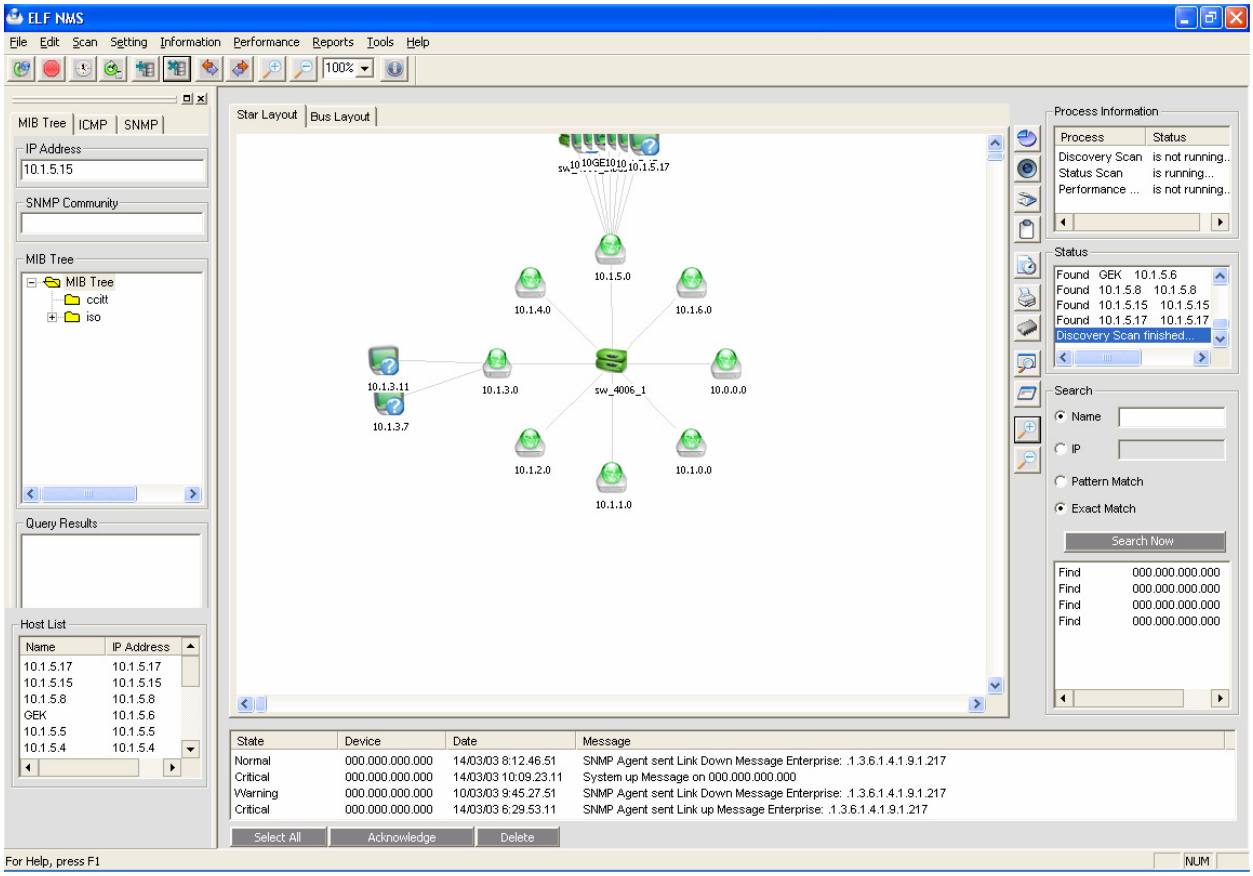
У NetCrunch очень много возможностей и я не могу описать их все в одной обзорной статье, поэтому я только описал и проиллюстрировал процесс автоматического сканирования сети. Преимуществ у этой проги достаточно много, а недостатков я заметил только два – нестабильность работы и неудобство редактирования структуры. За два дня NetCrunch трижды улетал в даун, что не очень приятно. Редактировать структуру сети тяжело, а некоторые вещи вообще невозможно сделать. Если учесть, что любое автоматическое сканирование допускает ошибки, то визуализация будет неточной.

ELF NMS

Где слить: http://www.secusis.com/

Вес: 2 метра

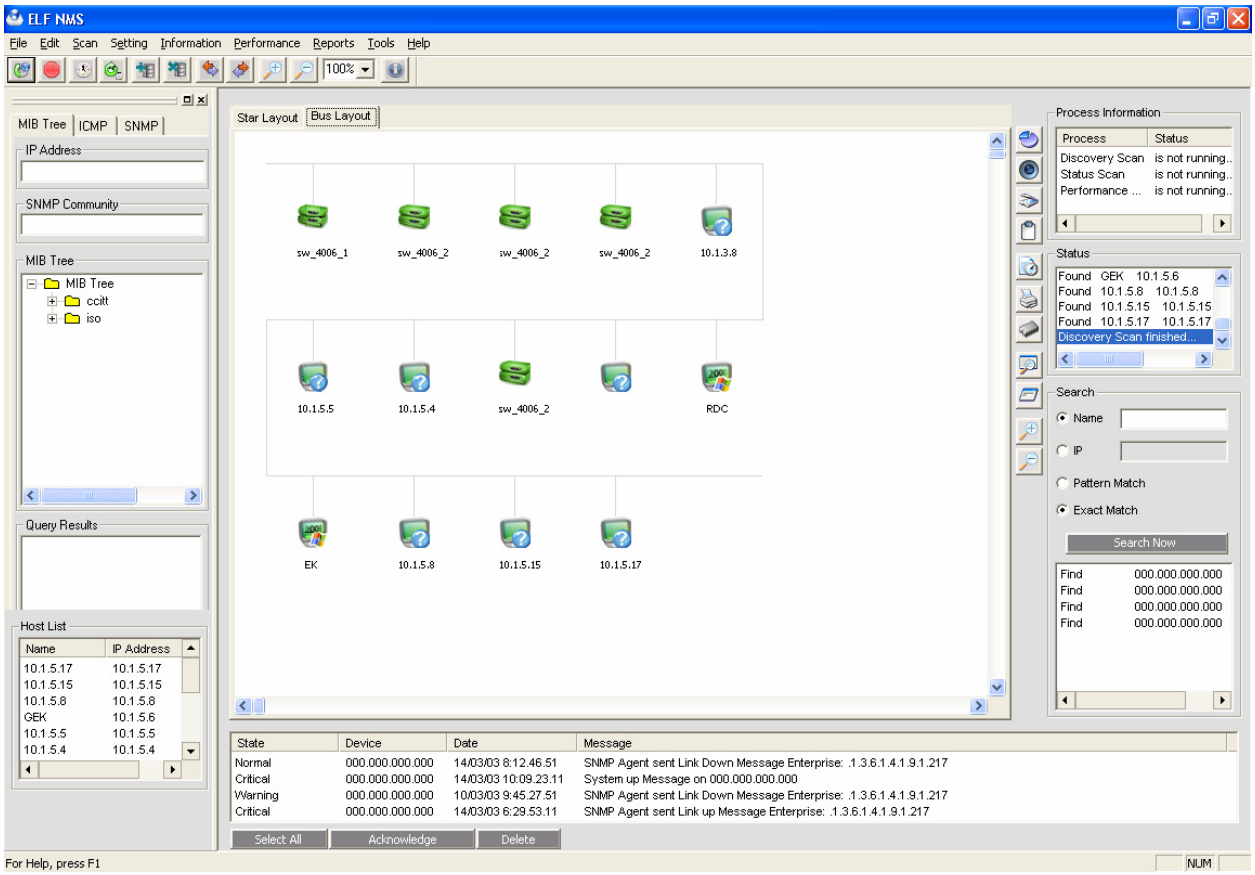
До недавнего времени (пока я не знал про NetCrunch) я использовал ELF NMS. Эта небольшая, но полезная в сканировании сети утилита более точно (по моей практике) создает визуальный вид сети, но меня бесит в ELF NMS отсутствие нормальной возможности редактирования компонентов сети. Несмотря на достаточно хорошую структурированность результата сканирования, иногда хочется какие-то компоненты передвинуть, чтобы лучше было видно входящие в сеть компьютеры.



Для сканирования сети достаточно выбрать из меню Scan пункт Start Scan и прога сама начинает сканировать сетку и добавлять найденные узлы в виде графических элементов в основное окно. Ищет она все правильно, но если в сети много коммутаторов, то разветвление может получиться не совсем точным. У меня она один коммутатор может втулить в несколько мест, хотя правильным будет только одно.

Просмотреть найденные устройства можно в двух режимах – звезда (Star Layout показан на рисунке 4) и шина (Bus Layout показан на рисунке 5). Это две основные и часто используемые топологии, которые может автоматически построить программа. От правильного выбора топологии зависит точность построения структуры сети. Сравни рисунки 4 и 5, на 4-м сеть более правдоподобна и выглядит красивее, хотя на самом

деле в моей сети используется топология кольца. Но за счет звездных разветвлений она отлично смотрится в виде Star Layout.



Если посмотреть на мою схему в виде Bus Layout, то сразу бросается в глаза повторяющееся устройство sw_4006_2. Это коммутатор и эта тулза просто размножила его в сети 4-е раза. Проблема в том, что к коммутатору подключено несколько сетей и ELF NMS и мне доступны только две из них, остальные запрещены (если быть точнее, то мне доступна была одна только сеть :)). Вместо того, чтобы добавить в график несколько сетей, я вижу множество коммутаторов, что очень даже мозолит глаза. Поэтому этой тулзе не хватает хорошего режима редактирования.

Еще один из недостатков ELF NMS, который меня просто бесит – несовместимость с интерфейсом MS. Простейший пример – прога не поддерживает подсказки и сколько я не наводил бы на кнопку, чтобы узнать зачем она нужна, ничего в строке состояния не отображалось, да и всплывающие подсказки отсутствуют. Так что разбираться с назначением кнопок на панели инструментов придется по картинкам (которые не очень информативны) или методом научного тыка.

Итог

На мой взгляд ELF NMS лучше отражает реальную структуру сети, по крайней мере в моей сети он более точен. NetCrunch – более мощный и содержит множество дополнительных возможностей для мониторинга сетевых ресурсов.

Раньше я для мониторинга сети использовал HostMonitor, а для автоматического сканирования сети ELF NMS, но теперь у меня есть NetCrunch, который практически сочетает в себе лучшие стороны обеих программ. Но ELF NMS остается в моем пакете незаменимым боевым товарищем, потому что в сканировании неизвестной мне сети он лучший, хотя и может запутать вставкой лишних коммутаторов туда, куда не надо.

Чего мне не хватает в обеих программах, так это точного определения ОС на сканируемом компьютере. Обе тулзы великолепно определяют Windows 2000, если на нем запущены сетевые сервисы FTP, HTTP. Определение ведется, видимо по приветственным сообщениям этих сервисов, поэтому если их отключить, то проги уже не определяют, что на компе стоит Win2k. Ну а такие вещи как XP и 2003 Server обе

тулзы просто не знают. Возможно, в следующих версиях эта проблема будет решена, потому что если админ знает ОСи на компьютерах своей сети, то нам приходится использовать для определения спец тулзы. Хорошо было бы встроить такую возможность прямо в анализатор сети.

Ну и на последок хочется пожелать тебе простой хакерской удачи!!!