

Lamescan 3

Руководство пользователя

Автор:
ТОВ. **redsh**

Изготовлено в СССР, 2010 г.

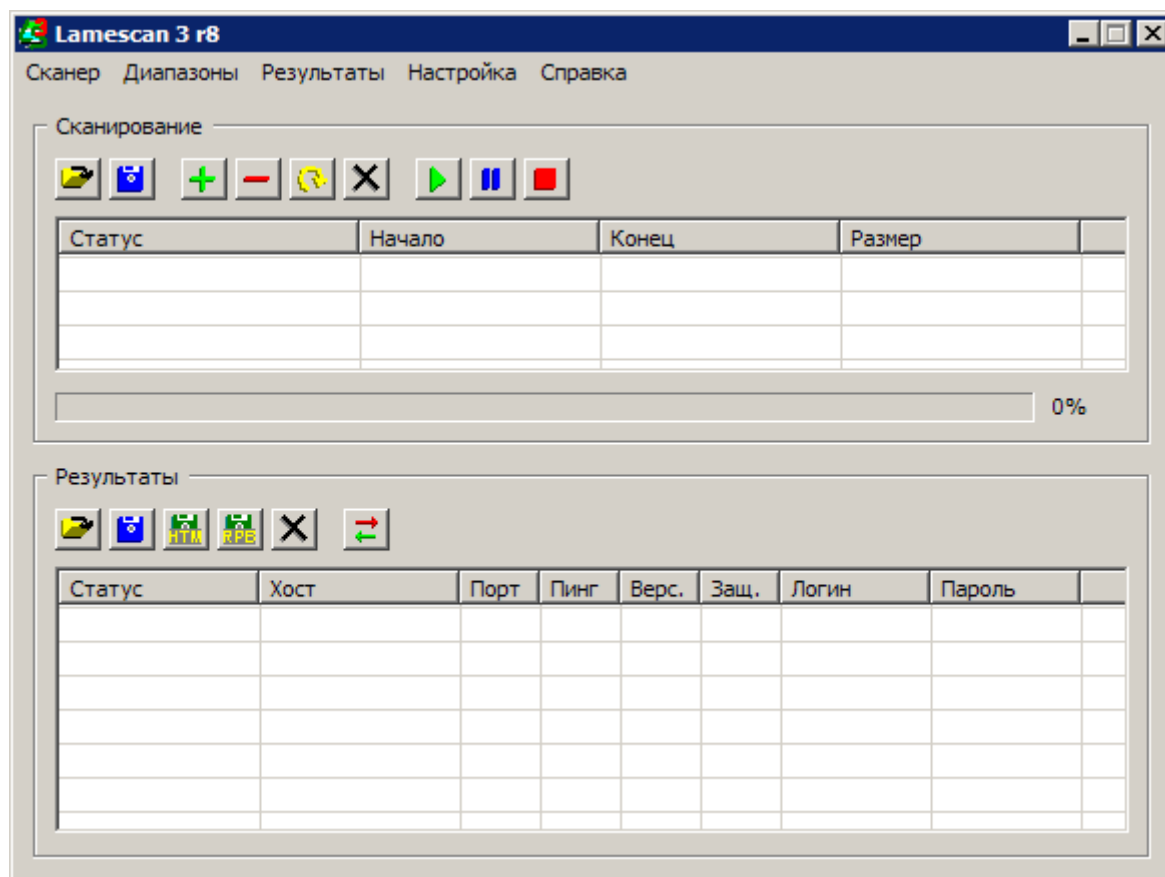
Краткая информация о Lamescan 3

Lamescan 3 – утилита для восстановления забытых паролей к проге Radmin Server со встроенным специализированным сканером портов. Утилита поддерживает следующий набор фич:

- Восстановление забытых паролей от Radmin Server 2.x, восстановление логинов и паролей от Radmin Server 3.x (методом брута по словарю), нахождение незапаролённых серверов Radmin.
- Многопоточное сканирование (с пинговкой) диапазона адресов с целью нахождения работающих серверов Radmin.
- Группировка сканируемого диапазона по категориям «В очереди» (ещё не просканированные хосты), «Просканировано» (обработанные хосты), «Оффлайн» (не пингующиеся на момент сканирования), «Ошибка» (хосты, при сканировании которых возникли сбои).
- Сохранение и загрузка сканируемого диапазона адресов в CSV (с возможностью продолжить с места сохранения). Импорт списка хостов (записанного в виде единичных адресов, диапазонов или CIDR-нотации).
- Экспорт результатов сканирования в CSV или HTML, импорт результатов сканирования из CSV (для просмотра).
- Поддержка SOCKS прокси-сервера (только для TCP-соединений).
- Возможность запуска клиента Radmin непосредственно из утилиты, без необходимости копировать результаты сканирования в контакт-лист Radmin Viewer.
- Автоматическая (или по запросу) проверка обновлений.
- Большинство параметров сканирования настраиваемы.

Мануал к проге Lamescan 3

Здесь приведено подробное руководство по успешному использованию Lamescan 3. Ниже ты видишь главное окно работающей тулзы, которой я воспользовался для восстановления забытых паролей от Radmin Server'ов установленных на двух виртуальных машинах.



Главное окно программы

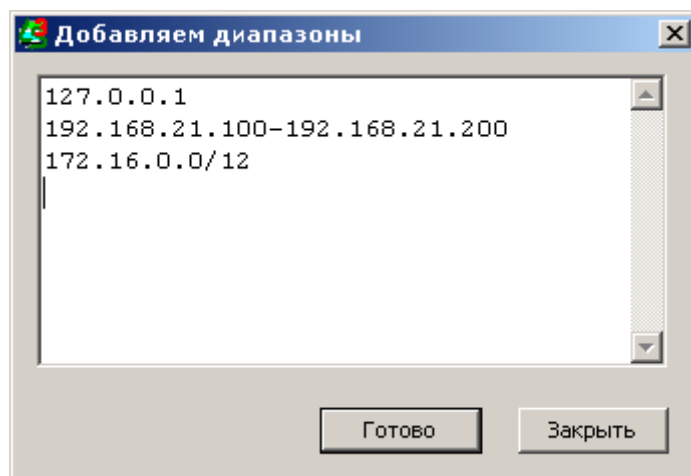
Добавление и удаление диапазонов

Lamescan 3 разработан для работы с большим количеством адресов, поэтому работа ведётся не с отдельными хостами (слишком медленно), а с диапазонами. Программа использует и показывает тебе диапазоны в виде промежутков адресов. Для добавления диапазона, нужно выбрать в меню программки «Диапазоны → Добавить в очередь → Список диапазонов», нажать Insert или кнопку «Добавить диапазоны».



Кнопочка «Добавить диапазоны»

Ты увидишь окно добавления диапазонов для сканирования. Можно добавить сколько угодно диапазонов, по одному на строку. Диапазоны могут быть записаны в виде единичных адресов, промежутков, или в CIDR-нотации:



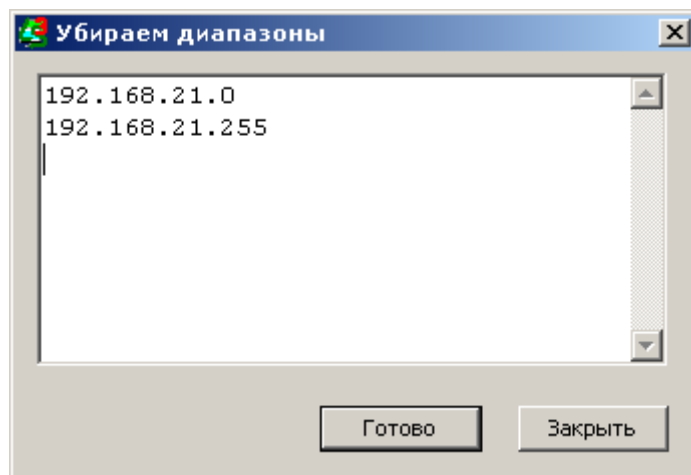
Добавление диапазонов

Подобным образом можно удалить диапазоны из таблицы. Для удаления, нужно выбрать в меню «Диапазоны → Удалить → Список диапазонов», нажать клавишу Delete или кнопку «Удалить диапазоны».



Кнопочка «Удалить диапазоны»

Отобразится окно, в котором можно ввести список диапазонов для удаления:



Удаление диапазонов

Очистить весь список диапазонов можно, выбрав в меню «Диапазоны → Удалить → Все», нажав комбинацию Ctrl+Delete или кнопку «Очистить список диапазонов».



Кнопочка «Очистить список диапазонов»

В главном окне программы можно видеть список диапазонов, с которыми ведётся работа:

Статус	Начало	Конец	Размер	
 В очереди	127.0.0.1	127.0.0.1	1	
 В очереди	172.16.0.0	172.31.255.255	1048576	
 В очереди	192.168.21.100	192.168.21.200	101	

Список диапазонов

Группы хостов

Lamescan 3 использует некое подобие базы данных хостов, в которой хранятся не просканированные, просканированные хосты и результат их сканирования. Добавляемые хосты попадают в группу «Очередь», хосты, которые не пингуются — в группу «Оффлайн», хосты с просканированными портами — в группу «Просканировано», хосты при сканировании которых возникли какие-то ошибки — в группу «Ошибка сканирования».

Статус	Начало	Конец	Размер	
 Ошибка сканир.	192.168.21.130	192.168.21.130	1	
 Просканирован	192.168.21.131	192.168.21.131	1	
 Оффлайн	192.168.21.132	192.168.21.132	1	

Группы хостов

Группы хостов удобны тем, что можно без труда повторить сканирование хостов, при первоначальном сканировании которых возникли ошибки, или которые были недоступны. Для добавления в очередь хостов из групп «Ошибка сканирования» и «Оффлайн», нужно выбрать в меню «Диапазоны → Добавить в очередь → Все «Оффлайн» и «С ошибками»», либо нажать комбинацию Ctrl+Insert, или кнопку «Повторить сканирование».



Кнопочка «Повторить сканирование»

Можно повторить сканирование любой из групп, выбрав соответствующий пункт в меню «Диапазоны → Добавить в очередь».

Загрузка и сохранение списка диапазонов

Список диапазонов можно сохранить, чтобы продолжить сканирование в дальнейшем. Сохранение ведётся в текстовый файл в формате CSV-таблицы (значения с разделителями, по одному диапазону на строку). Диапазоны из одного хоста сохраняются одним значением, из нескольких — двумя значениями (начало и конец), следующее значение может быть «off», «on» или «error» в зависимости от группы (соответственно «Оффлайн», «Просканировано», «Ошибка»). По умолчанию диапазоны относятся к группе «Очередь». Для сохранения таблицы, можно выбрать в меню пункт «Диапазоны → Сохранить», клавишу F2, или кнопку «Сохранить диапазоны».



Кнопочка «Сохранить диапазоны»

Загрузка таблицы диапазонов осуществляется выбором пункта меню «Диапазоны → Загрузить», нажатием клавиши F3 или кнопки «Загрузить диапазоны». При этом, загруженная таблица добавляется к текущей таблице.



Кнопочка «Загрузить диапазоны»

Запуск и остановка сканирования

Для запуска сканирования диапазонов, нужно выбрать в меню «Сканер → Пуск», нажать F5 или кнопку «Пуск». Для остановки сканирования - «Сканер → Стоп» в меню, F6 или кнопку «Стоп». Чтобы временно приостановить сканирование, можно нажать «Сканер → Пауза», F8 или кнопку «Пауза» (продолжить можно снова нажав «Пауза» или «Пуск»).



Кнопочки «Пуск», «Пауза» и «Стоп»

При сканировании, хосты перемещаются из группы «Очередь» в другие группы, в соответствии с результатом сканирования. При прерывании сканирования, хосты, которые обрабатывались в момент прерывания попадают в группу «Ошибка сканирования».

Работа с результатами сканирования

В результаты сканирования попадают хосты, на которых обнаружен работающий сервер Radmin. Таблицу результатов можно сохранить и загрузить в виде CSV-таблицы, соответственно выбрав в меню «Результаты → Сохранить», «Результаты → Загрузить», нажав комбинации Shift+F2 или Shift+F3, или кнопки «Сохранить результаты» или «Загрузить результаты».



Кнопочки «Загрузить результаты» и «Сохранить результаты»

Таблицу результатов можно экспортировать в виде HTML-таблицы, выбрав в меню «Результаты → Экспорт в HTML», нажав F7 или кнопку «Экспорт результатов в HTML».



Кнопочка «Экспорт результатов в HTML»

Также, можно экспортировать таблицу результатов в виде адресной книги Radmin, для этого выбери в меню «Результаты → Экспорт в RPB», нажми Shift+F7 или кнопку «Экспорт результатов в RPB».



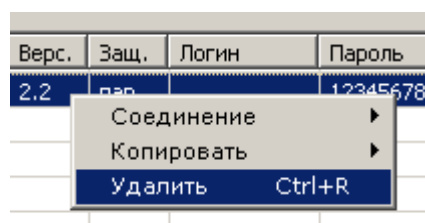
Кнопочка «Экспорт результатов в RPB»

Очистить таблицу результатов можно, выбрав в меню «Результаты → Очистить», нажав Shift+Delete или кнопку «Очистить таблицу результатов».



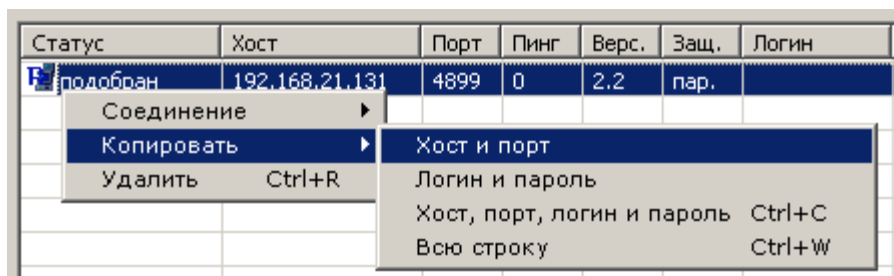
Кнопочка «Очистить таблицу результатов»

Таблицу результатов можно сортировать по определённому столбцу, кликнув соответствующий заголовок столбца. Удалить определённый результат из таблицы, можно выделив результат и нажав Ctrl+R, либо выбрать в контекстном меню таблицы результатов «Удалить».



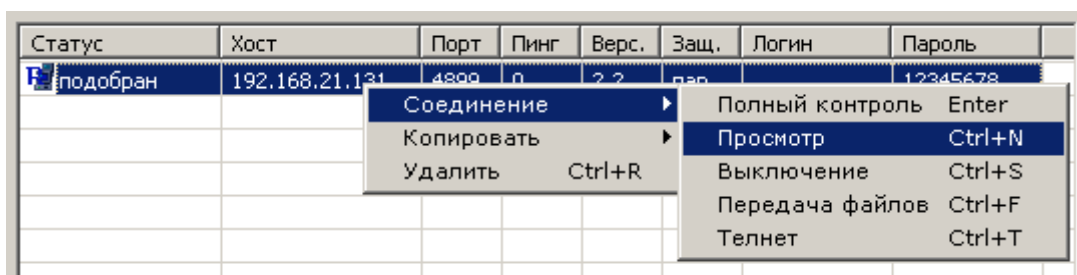
Удаление результата из таблицы

Скопировать значения из таблицы результатов в буфер обмена, можно выбрав пункт «Копировать» из контекстного меню результатов, либо нажав «Ctrl+C» для копирования адреса хоста, порта Ramin Server'a, логина и пароля, либо «Ctrl+W» для копирования всей информации о хосте.



Копирование информации о результате сканирования хоста

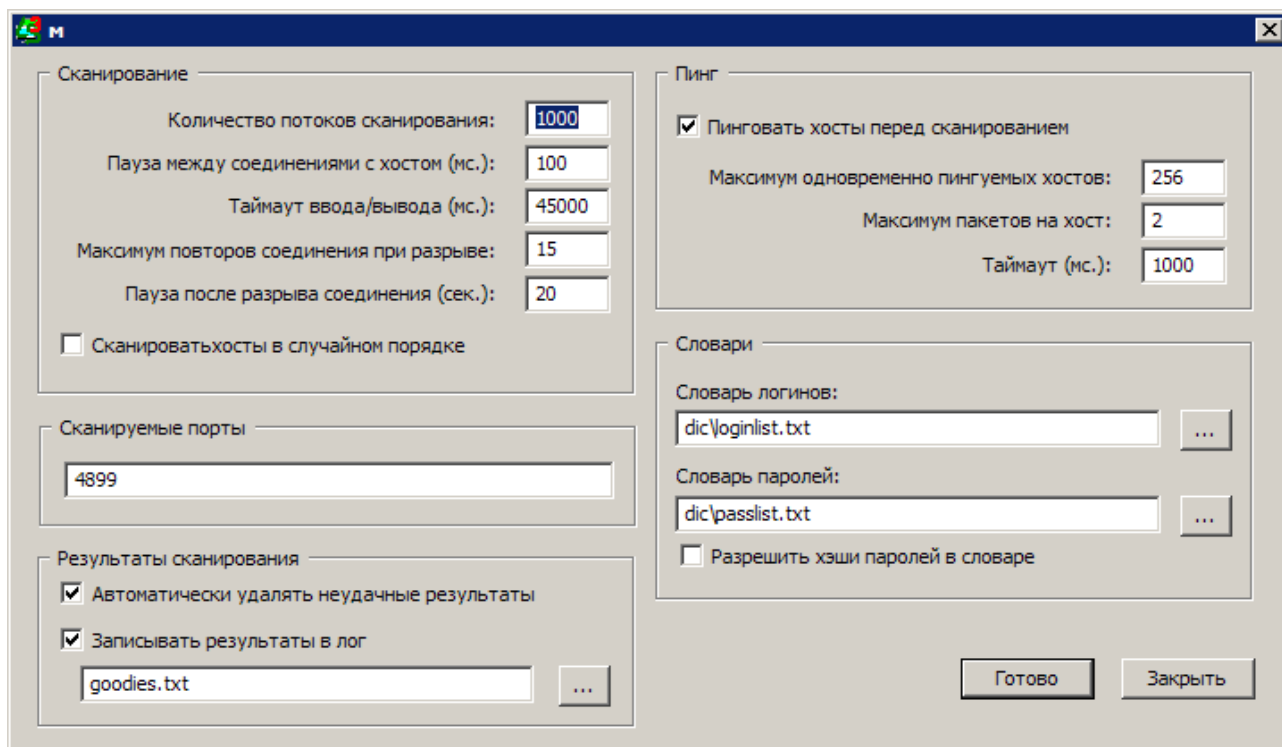
Также, для результата сканирования можно запустить Radmin Viewer. Для этого можно выбрать пункт «Соединение» в контекстном меню результата, либо нажав клавиши Enter, Ctrl+N, Ctrl+S, Ctrl+F или Ctrl+T соответственно для соединения в режиме «Полный контроль», «Только просмотр», «Выключение», «Передача файлов» или «Telnet». Также, запустить Radmin Viewer для хоста в режиме «Полный контроль» можно двойным кликом мыши по строке таблицы результатов.



Запуск Radmin Viewer'a для определённого результата сканирования

Настройка сканирования

Для доступа к настройкам сканирования, нужно выбрать в меню программы «Настройка → Основное» или нажать клавишу F9. Настройка сканирования выполняется с помощью такого диалога:



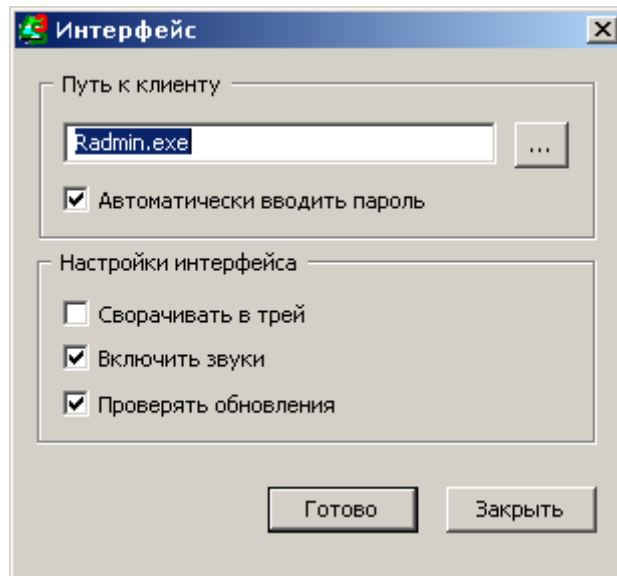
Диалог настройки сканирования

Словари логинов и паролей

Словари хранятся в текстовом файле, по одному логину или паролю в строке. Логины используются только при работе с Radmin 3.x. В словаре паролей могут содержаться md5-хэши от 100 байт пароля, дополненного нулями. Если опция "Разрешить хэши паролей в словаре" включена, подходящие строки будут считаться хэшами и использоваться при работе с Radmin 2.x, если эта опция выключена, все строки будут считаться паролями.

Настройка интерфейса

Для доступа к настройкам интерфейса, нужно выбрать в меню программы «Настройка → Интерфейс» или нажать Shift+F9.



Диалог настройки интерфейса

Путь к клиенту — здесь указывается расположение Radmin Viewer'a для запуска из списка результата. Опция «Автоматически вводить пароль» указывает, следует ли автоматически отвечать на запросы Radmin Viewer'a о вводе логина и пароля.

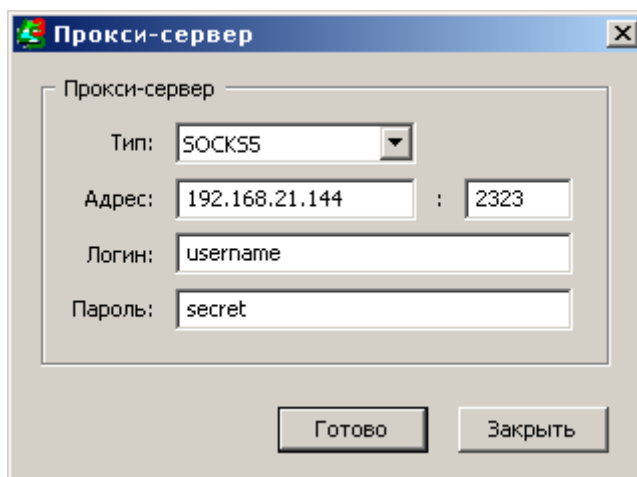
Сворачивать в трей — указывает, следует ли скрывать окно и добавлять значёк в трее при сворачивании окна программы для экономии места в таскбаре.

Включить звуки - указывает, следует ли воспроизводить звуковые сигналы при нахождении сервера и завершении сканирования.

Проверять обновления — указывает, стоит ли обращаться к серверу обновлений через каждые 5 запусков программы для поиска свежих версий.

Использование прокси-сервера

Прокси сервер используется только для TCP-соединений с Radmin Server'ом. ICMP-запросы и проверка обновлений осуществляется прямым соединением. Если осуществлять прямые запросы нежелательно, следует отключить пинг перед сканированием и автоматическую проверку обновлений. Для доступа к настройкам сервера, нужно выбрать в меню программы пункт «Настройка → Прокси-сервер» или нажать Ctrl+P.



Диалог настройки прокси-сервера

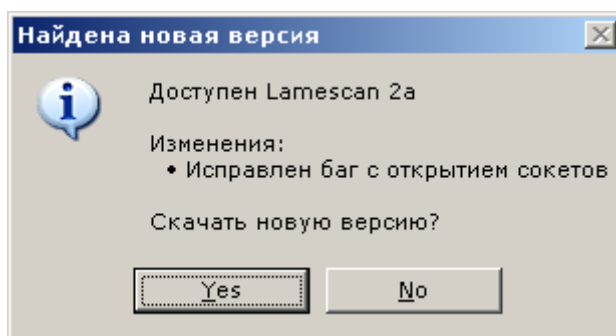
Тип — указывает стоит ли использовать прокси и тип прокси. Поддерживаются SOCKS4 и SOCKS5 прокси, для SOCKS5 поддерживается соединение с авторизацией логином/паролем и без авторизации.

Адрес — указывается адрес и порт прокси-сервера.

Логин и пароль — данные для авторизации при использовании SOCKS5-прокси.

Проверка обновлений

Проверка обновления происходит при каждом шестом запуске программы, если данная опция включена в настройках или вручную, выбором в меню программы команды «Справка → Проверить обновления». При наличии новых обновлений, выводится сообщение, отображающее последнюю версию и список изменений и предлагается скачать свежую версию.



MessageBox с информацией об обновлении

Работа в Wine

В данный момент известна следующая проблема с совместимостью, возникающая при использовании Wine. Lamescan 3 использует библиотеку `icmpapi.dll`, из которой успешно вызывать функции в винде может любой пользователь (на этой библиотеке основана штатная виндовая тулза `ping`). В Wine эта библиотека реализована через равсокет, которые для открытия требуют соответствующих привилегий. Если запускать прогу без права открытия равсокета, сканируемые хосты пинговаться не будут. Самое простое решение — запускать Wine с правами суперюзера: (`sudo wine lamescan3.exe`). Если это не приемлемо по соображениям безопасности, придётся отключить пинговку хостов в настройках (Настройка → Основное → Пинговать хосты перед сканированием).