## Сканер Nessus

### Введение

Выше рассматривались основные принципы анализа защищённости, методы тестирования различных служб, были приведены примеры инструментов для проведения тестов. Сканеры безопасности, рассматриваемые далее, сочетают в себе возможности отдельных инструментов и реализуют различные методы сканирования. В данном модуле рассматривается сетевой сканер Nessus.

### Обзор возможностей сканера Nessus

Nessus – это сканер уязвимостей, который может быть использован для сканирования одного или нескольких узлов сети. Это свободно распространяемый инструмент сканирования с регулярно обновляемой базой проверок. Далее перечислены его основные характеристики и возможности:

1. **Модульная архитектура**. Каждая проверка, выполняемая сканером Nessus**,** представляет собой внешний модуль (plugin). Это позволяет легко добавлять новые проверки. Полный список имеющихся проверок может быть найден по адресу: http://cgi.nessus.org/plugins.
2. **Язык NASL**. Сканер Nessus имеет встроенный язык описания проверок (NASL, Nessus Attack Scripting Language), позволяющий создавать пользовательские проверки. Проверки могут быть написаны и на языке C.
3. **Регулярно обновляемая база проверок**. Проверки новых уязвимостей могут добавляться каждый день.
4. **Распределённая архитектура (клиент/сервер)**. Сканер Nessus состоит из двух частей: сервера, выполняющего проверки и клиента, предоставляющего пользовательский интерфейс. Эти части могут быть распределены по нескольким узлам. Таким образом, можно выполнять сканирование большой сети, управляя процессом с одного рабочего места.
5. **Параллельное сканирование нескольких узлов сети**. Возможности по одновременному сканированию ограничены лишь производительностью узла, на котором запущена серверная часть сканера.
6. **Идентификация служб**. Сканер Nessus учитывает, что службы могут использовать нестандартные порты.
7. **Сканирование нескольких одинаковых служб, находящихся на одном узле**. Если, например, на узле имеется два web-сервера (использующие разные номера портов), сканер Nessus будет выполнять проверки в отношении каждого из них.
8. **Система генерации и экспорта отчётов.** Отчёты содержат подробное описание уязвимостей и рекомендации по их устранению. Клиентская часть сканера Nessus имеет возможности экспорта отчётов в различные форматы (ASCII text, LaTeX, HTML, HTML с графикой).
9. **Динамическое подключение/выключение проверок.** Сканер Nessus использует результаты уже проделанных проверок для выполнения следующих. В зависимости от результатов этапа сбора информации, ненужные проверки могут быть выключены.

### Архитектура сканера Nessus

Сканер Nessus состоит из двух частей: Nessus-сервер и Nessus-клиент. Это сканер сетевого уровня, выполняющий дистанционные проверки. Серверная часть может работать на любой UNIX-платформе (FreeBSD, Linux, BSDI, Solaris и другие). Клиентская часть может работать на различных платформах (имеются клиенты для X11 и Win32).



В зависимости от задач и сетевого окружения можно предложить различные варианты расположения серверных и клиентских частей. Иногда бывает удобно иметь переносной компьютер с клиентской и серверной частями сканера Nessus, подключать его к различным участкам сети и проводить сканирование. Иногда, для сканирования различных участков сети с разных точек зрения, целесообразно установить несколько серверных частей сканера Nessus и управлять ими с помощью одного клиента.



При проведении сканирования несколькими пользователями можно использовать одну серверную часть сканера, подключаясь к ней с различных клиентов.

Для защиты взаимодействия между клиентской и серверной частями используется SSL.

### Получение и установка сканера Nessus

Получение дистрибутива

Дистрибутив сканера Nessus может быть получен по адресу: **http://www.nessus.org.** в виде сценария **nessus-installer.sh.** Дополнительнопотребуется скачать файл MD5.txt, содержащий контрольную сумму. Эти два файла необходимо поместить в какой-либо каталог (например, /root/soft/nessus) на том узле, где планируется развернуть серверную часть. По этому же адресу может быть получен и клиент Win32.

Установка

Далее необходимо перейти в каталог с полученным дистрибутивом сканера и запустить установку командой: **sh nessus-installer.sh**. В процессе установки потребуется ответить на ряд вопросов, и через некоторое время серверная часть (а также клиент для Х11) будет установлена. После установки к переменной $PATH будут добавлены записи:

"/usr/local/bin"

"/usr/local/sbin"

Для проверки можно воспользоваться командой "echo $PATH".

Кроме того, в файл /etc/ld.so.conf необходимо добавить строку "/usr/local/lib, а затем запустить ldconfig (это также делается в процессе установки).

После установки необходимо выполнить ряд действий по подготовке серверной части:

1. Создать сертификат сервера командой nessus-mkcert. Это необходимо для защиты взаимодействия между клиентом и сервером Nessus.
2. Добавить пользователя для подключения со стороны клиента (локального или удалённого) командой nessus-adduser

Удаление сканера Nessus

Для удаления сканера необходимо выполнить команду

uninstall-nessus.

Затем, возможно, потребуется вручную удалить некоторые каталоги и файлы (можно воспользоваться поиском по ключевому слову «nessus»).

Запуск сканера Nessus

Запуск серверной части

Серверная часть сканера может быть запущена командой

#nessusd -D

При этом параметры задаются в файле **/usr/local/etc/nessus/nessusd.conf**

Запуск клиентской части

Для запуска интерфейса сканера (должна быть загружена графическая оболочка) необходимо в командной строке набрать:

#nessus

Обновление базы проверок

Обновление вручную

Для подключения новых внешних модулей необходимо:

1. Скопировать их с web-сервера http://www.nessus.org в каталог .../nessus/lib/nessus/plugins.
2. Завершить выполнение процесса nessusd:   
   kill -9 <pid>, где pid - идентификатор процесса nessusd.
3. Вновь запустить сервер nessusd с помощью команды nessusd –D.

После запуска сервера новые модули будут доступны для проведения проверок с их использованием.

Автоматически через Internet

Для этого на узле должны быть установлены:

1. Lynx,
2. tar,
3. gzip

Обновление осуществляется с помощью команды nessus-update-plugins. При этом осуществляется подключение к сайту [www.nessus.org](http://www.nessus.org) и скачивание новых проверок.

Если подключение осуществляется через proxy-сервер, потребуется создать файл в домашнем каталоге пользователя с именем .nessus-update-pluginsrc, где и указать необходимые параметры. Например, файл может содержать следующие строки:

proxy\_user=root

proxy\_passwd=qwerty

proxy=200.4.4.254:8080.

### Практическая работа Подготовка сканера Nessus к работе.

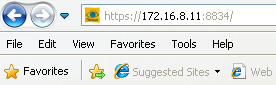


Серверная часть сканера Nessus запускается на виртуальной машине с ОС **Linux**, клиентская часть запускается на виртуальной машине Windows XP.

1. Загрузить виртуальную машину с ОС **Linux.**
2. Войти в систему
3. Установить сканер Nessus, если он не установлен (уточнить у преподавателя).
4. Запустить серверную часть **nessusd.**service **nessusd start**



1. Перейти в виртуальную машину Windows XP
2. Запустить Internet Explorer
3. В адресной строке указать https://172.16.8.11:8834



1. Ввести учётные данные пользователя (adm, 1111) и нажать Log in



1. Убедиться, что соединение установлено

### Работа со сканером Nessus

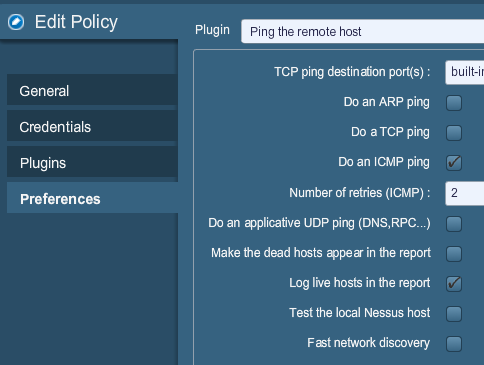
Сбор информации о сканируемой сети

Вне зависимости от выбранного варианта сканирования (тестирование на устойчивость к взлому снаружи или аудит внутренней сети) необходим сбор начальной информации о сканируемой сети. Для этого можно использовать рассмотренные выше способы и средства, но, как правило, сканеры уязвимостей имеют встроенные возможности инвентаризации сетевых ресурсов. Далее рассматриваются возможности сканера Nessus по идентификации узлов сети и служб [21].

Идентификация узлов

Nessus поддерживает четыре способа идентификации узлов:

1. ARP Ping
2. ICMP Ping
3. ТСР Ping
4. UDP Discovery



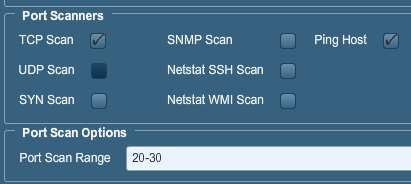
Сканирование портов

Следующий шаг – поиск работающих на узле сетевых служб. Это типичный шаг для большинства сканеров уязвимостей. Следует понимать, что переход к этому шагу сканер осуществляет лишь в том случае, если узел по результатам предыдущего шага был признан доступным.

Nessus использует два метода сканирования портов:

1. TCP Scan– сканирование с установлением соединения
2. SYN Scan – сканирование без установления соединения

Оба эти метода рассматривались выше. Их можно включить через закладку «Port Scanners»:

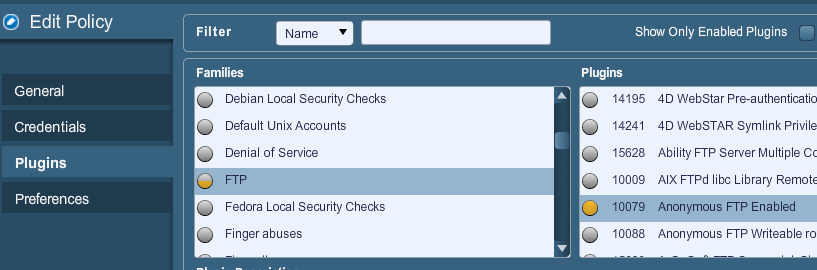


Для проведения сканирования портов UDP необходимо использовать опцию UDP Scan.

Результат данного этапа – список открытых портов на сканируемом узле (найденных на основе указанных настроек).

Выбор проверок

Последний шаг – выбор проверок для сканирования узла. Их можно включить/выключить в секции Plugins.



### Практическая работа Сбор информации о сети с помощью сканера Nessus.

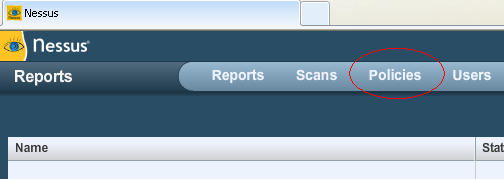


Цель работы – изучение методов сбора информации о сканируемой сети, встроенных в Nessus. Серверная часть сканера Nessus запускается на узле с ОС Linux, клиентская часть запускается на обоих узлах пары.

Идентификация узлов

Цель – поиск активных узлов в сети, заданной преподавателем.

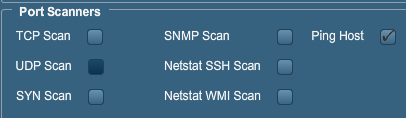
1. Узнать у преподавателя диапазон сканируемых узлов  
     
   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Перейти по ссылке «Policies»



1. Нажать кнопку Add
2. Указать имя политики сканирования, например, Network Discovery



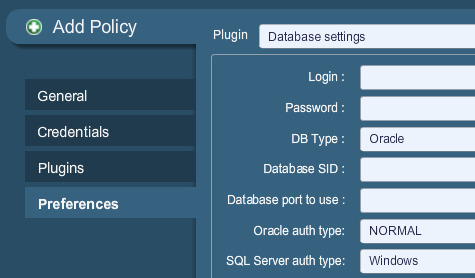
1. Отключить все опции в секции Port Scanners, кроме Ping Host



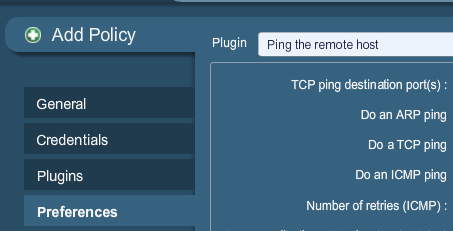
1. Перейти к области Plugins



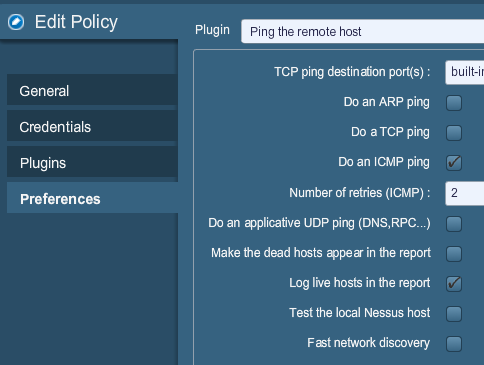
1. Оключить все проверки (нажать Disable All)
2. Перейти к области Preferencies



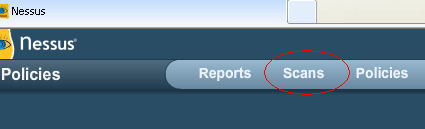
1. Открыть группу параметров Ping the remote host



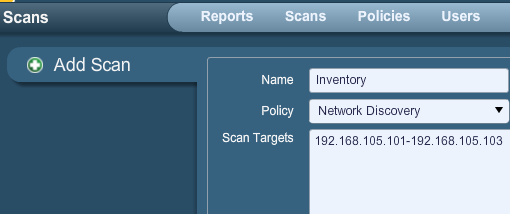
1. Отключить все опции, кроме ICMP Ping и Log live hosts in the report



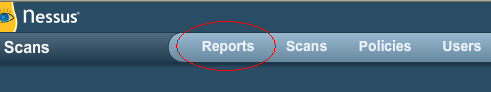
1. Сохранить политику сканирования, нажав Submit
2. Перейти по ссылке «Scans»



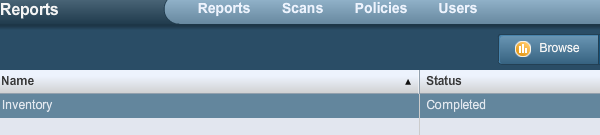
1. Нажать Add
2. Выбрать созданную ранее политику сканирования, указать название сканирования, указать диапазон сканируемых узлов



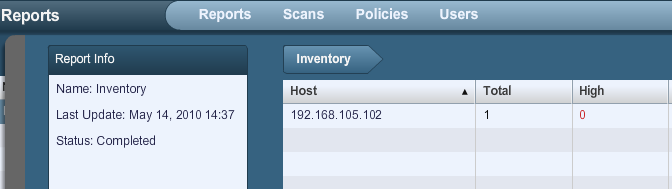
1. Нажать кнопку Launch Scan
2. Дождаться окончания процесса сканирования (около 1 минуты) и перейти по ссылке Reports



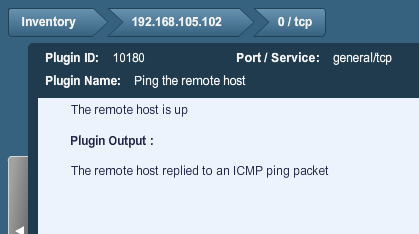
1. Выбрать результаты сканирования и нажать Browse



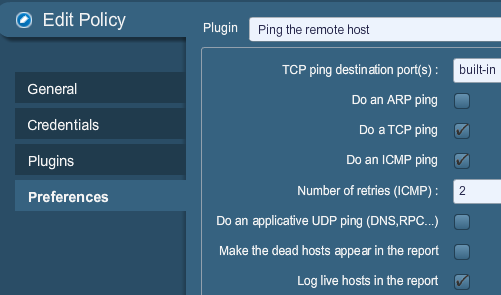
1. Обратить внимание на найденные узлы (должен быть найден один узел):



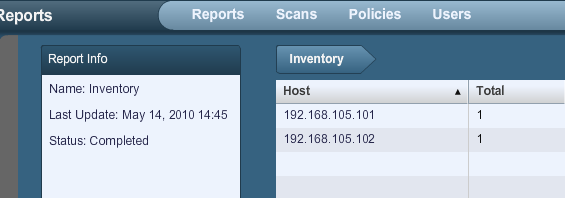
1. Просмотреть более подробную информацию



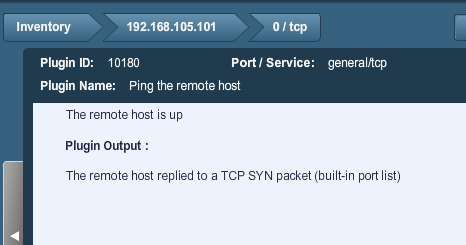
1. Перейти к редактированию политики сканирования и включить метод TCP Ping



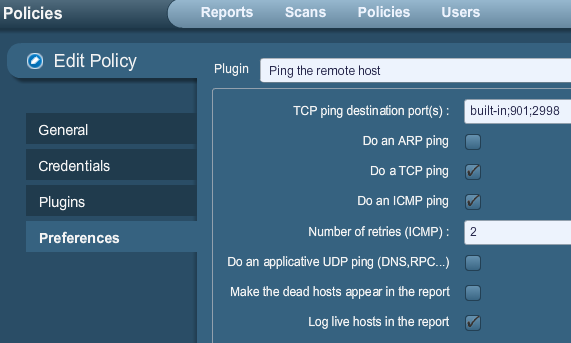
1. Сохранить политику и вновь произвести сканирование сети. Обратить внимание на найденные узлы (должно быть найдено два узла)



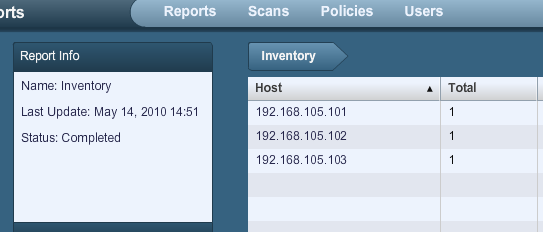
1. Просмотреть более подробную информацию по одному из узлов



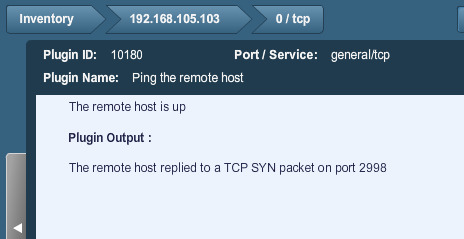
1. Перейти к редактированию политики сканирования и для метода TCP Ping задать порты 901 и 2998



1. Вновь произвести сканирование сети. Обратить внимание на найденные узлы (должно быть найдено три узла).



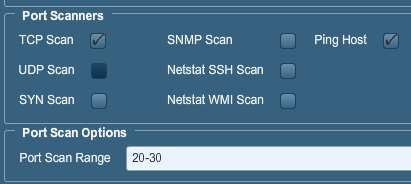
1. Просмотреть более подробную информацию по узлу 192.168.х.103, обратить внимание на порт, использованный методом TCP Ping



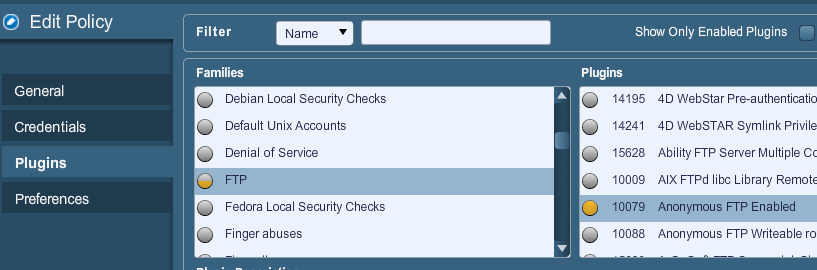
Сканирование портов и идентификация служб

Цель – получение списка активных служб. Производится сканирование виртуальной машины Windows.

1. Включить виртуальную машину Windows
2. Войти в систему, уточнить IP-адрес.
3. В сканере Nessus открыть для редактирования ранее созданную политику сканирования
4. В секции «Port Scanners» включить TCP Scan и задать диапазон портов, подлежащих сканированию: 20-30



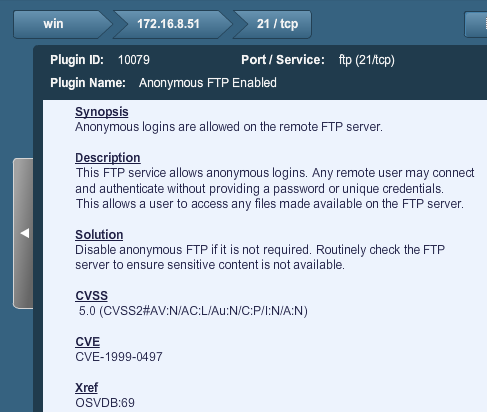
1. Перейти к области Plugins
2. Включить проверку Anonymous FTP enabled



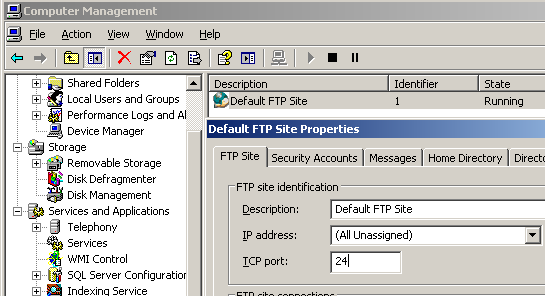
1. Произвести сканирование виртуальной машины Windows



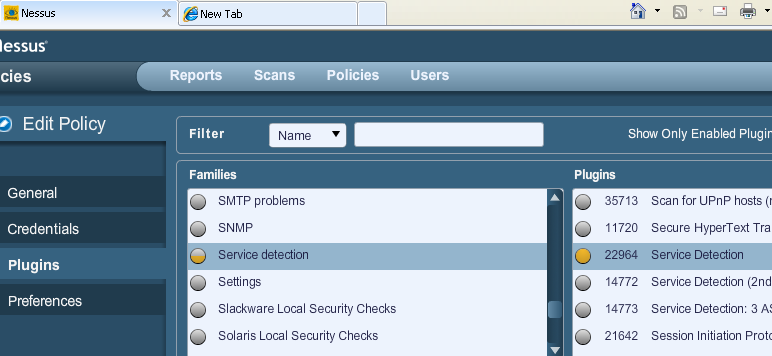
1. Проанализировать результаты (на узле должен быть обнаружен анонимный FTP-сервер).



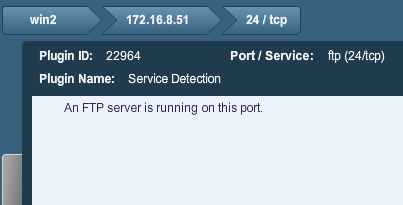
1. На узле с ОС Windows задать для сервера ftp номер порта 24 (вместо 21)



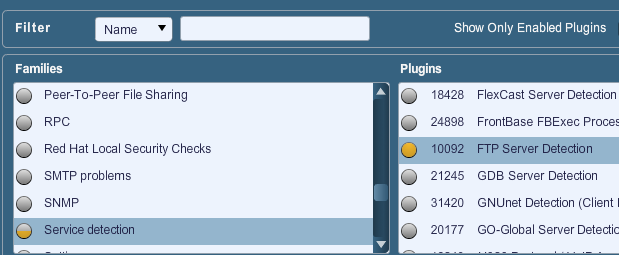
1. Перезапустить FTP сервер
2. Вновь произвести сканирование узла с ОС Windows
3. Проанализировать результаты (на узле всё равно должен быть обнаружен анонимный FTP-сервер).
4. Включить проверку «service detection».



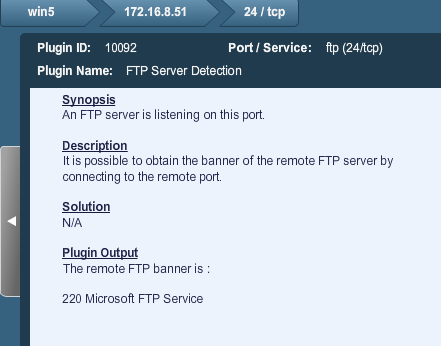
1. Произвести сканирование узла с ОС Windows
2. Проанализировать результаты (среди них найти информацию об идентификации сервисов).



1. Включить проверки «FTP server detection» и «SMTP server detection»



1. Произвести сканирование узла с ОС Windows
2. Проанализировать результаты идентификации приложения



1. Включить проверку OS Identification



1. Произвести сканирование узла
2. Проанализировать результаты идентификации ОС, обратить внимание на использованный метод

