МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__» _____ 2017г.

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ СЕТЕВЫХ ПОРТОВ

Методические указания по выполнению лабораторных работ по дисциплине «Проектирование защищенных телекоммуникационных систем» для студентов специальности 10.05.02

Курск 2017

УДК 004.056.55

Составитель А.Л. Марухленко

Рецензент
Кандидат технических наук, доцент *И.В. Калуцкий*

Устранение уязвимостей сетевых портов: методические указания по выполнению лабораторных работ по дисциплине «Проектирование защищенных телекоммуникационных систем»/ Юго-Зап. гос. ун-т; сост. А.Л. Марухленко. Курск, 2017. - 10с.

Рассматриваются особенности протокола NetBIOS. Указывается порядок выполнения лабораторной работы, теоретические сведенияи необходимый для выполнения перечень литературы.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальности 10.05.02.

Текст печатается в авторской редакции

Подписано в печать 01.11.2017. Формат 60x84 1/16.
Усл.печ. л. 0,6. Уч.-изд.л. 0,5. Тираж 30 экз. Заказ _____. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ЦЕЛЬ РАБОТЫ**Ошибка! Закладка не определена.**

ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ**Ошибка! Закладка не определена.**

ЗАДАНИЕ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ**Ошибка! Закладка не определена.**7

БИБЛИОГРАФИЧЕСКИЙ СПИСОК**Ошибка! Закладка не определена.**0

ЦЕЛЬ РАБОТЫ

По результатам сканирования сетевых портов на машине с установленным брандмауэром, произвести его настройку для скрытия или устранения найденных уязвимостей.

ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

Выполнение данной лабораторной работы заключается в том, чтобы правильно настроить брандмауэр для устранения или скрытия найденных ранее уязвимостей. Данная работа посвящена настройке правил реагирования брандмауэра на различные события. Для выполнения работы необходимо изучить и освоить работу брандмауэра. Agnitum Outpost Firewall Pro версии 4.0

Протокол NetBIOS был создан для работы в локальных сетях. Система NetBIOS предназначена для персональных ЭВМ типа IBM/PC в качестве интерфейса, независящего от фирмы-производителя. NetBIOS использует в качестве транспортных протоколов TCP и UDP. Описание NetBIOS содержится в документе IBM 6322916 "Technical Reference PC Network".

Пакет NETBIOS создан для использования группой ЭВМ, поддерживает как режим сессий (работа через соединение), так и режим дейтограмм (без установления соединения). 16-и символьные имена объектов в netbios распределяются динамически. netbios имеет собственную dns, которая может взаимодействовать с интернетовским. Имя объекта при работе с NETBIOS не может начинаться с символа *.

Приложения могут через netbios найти нужные им ресурсы, установить связь и послать или получить информацию. NETBIOS использует для службы имен порт - 137, для службы дейтограмм - порт 138, а для сессий - порт 139.

Любая сессия начинается с netbios-запроса, задания ip-адреса и определения tcp-порта удаленного объекта, далее следует обмен NETBIOS-сообщениями, после чего сессия закрывается. Сессия

осуществляет обмен информацией между двумя netbios-приложениями. Длина сообщения лежит в пределах от 0 до 131071 байт. Допустимо одновременное осуществление нескольких сессий между двумя объектами.

При организации IP-транспорта через NETBIOS IP-дейтограмма вкладывается в NETBIOS-пакет. Информационный обмен происходит в этом случае без установления связи между объектами. Имена Netbios должны содержать в себе IP-адреса. Так часть NETBIOS-адреса может иметь вид, ip.**.**.**.**, где IP указывает на тип операции (IP через Netbios), а **.**.**.** - ip-адрес. Система netbios имеет собственную систему команд (call, listen, hang up, send, receive, session status, reset, cancel, adapter status, unlink, remote program load) и примитивов для работы с дейтограммами (send datagram, send broadcast datagram, receive datagram, receive broadcast datagram). Все оконечные узлы netbios делятся на три типа: широковещательные ("b") узлы; узлы точка-точка ("p"); узлы смешанного типа ("m").

IP-адрес может ассоциироваться с одним из указанных типов. B-узлы устанавливают связь со своим партнером посредством широковещательных запросов. P- и M-узлы для этой цели используют netbios сервер имен (NBNS) и сервер распределения дейтограмм (NBDD).

После сканирования удаленной виртуальной машины с установленным брандмауэром со стандартными настройками, сканер находит несколько уязвимостей, в том числе, и уязвимость по сессии NetBIOS на 139 порту. Для устранения данной проблемы необходимо использовать обходной путь, потому что «грубо» этот порт закрыть нельзя. Чтобы устранить проблему 139-го порта, необходимо определить доверенную группу IP-адресов, члены которой смогут взаимодействовать по сети. Для других уязвимых портов необходимо создать правило реагирования брандмауэра. Глобальные правила брандмауэра применяются ко всем процессам и приложениям на вашем компьютере, которые запрашивают доступ в сеть. Например, создав соответствующие правила, вы можете блокировать весь трафик, идущий по данному протоколу или с данного удаленного узла. Некоторые из установок глобальных правил, подобранные оптимальным образом, Outpost Firewall Pro задает по умолчанию.:

Каждый компьютер в локальной сети может получить один из трех уровней доступа к компьютеру:

- NetBIOS. Разрешает разделение доступа к файлам и принтерам между компьютером из локальной сети и вашим компьютером. Чтобы установить этот уровень, отметьте соответствующий флажок NetBIOS для этого адреса;

- Доверенные. Все соединения к и из этой сети разрешены. Чтобы установить этот уровень, отметьте флажок Доверенные для этого адреса;.

- Ограниченный доступ к LAN. NetBIOS соединения блокируются, все остальные соединения обрабатываются, согласно глобальным правилам и правилам для приложений. Чтобы установить этот уровень, уберите оба флажка NetBIOS и Доверенные для этого адреса.

Важно помнить, что узел, относящийся к числу Доверенных, имеет наивысший приоритет. С таким узлом могут соединяться даже запрещенные приложения. Рекомендуется помещать в список Доверенных только СОВЕРШЕННО БЕЗОПАСНЫЕ компьютеры. Если вам нужно только разделение доступа к файлам и принтерам, лучше использовать уровень NetBIOS, а не Доверенные. Нажав на кнопку «добавить», в обработку можно включить как отдельный IP-адрес, так и диапазон IP-адресов или отдельный домен.

Одной из наиболее важных характеристик системы Agnitum Outpost Firewall Pro является политика или режим работы с сетью. Существует пять режимов или политик с сетью.

Режим бездействия (Отключить) – разрешены все сетевые взаимодействия; брандмауэр отключен.

Режим разрешения (Разрешить) – разрешены все сетевые взаимодействия, которые явно не заблокированы.

Режим обучения (Обучения) – первое сетевое взаимодействие каждого приложения сопровождается предупреждением и дает вам возможность создать правило для работы этого приложения с сетью. Созданное правило будет немедленно задействовано брандмауэром для обработки соединений.

Режим блокировки (Блокировать) – запрещены все сетевые взаимодействия, за исключением явно разрешенных. Для каждого приложения, которому необходим доступ в Интернет, потребуется создать правило брандмауэра.

Блокировать все (Запрещать) – запрещены сетевые взаимодействия.

Сразу после установки программа по умолчанию функционирует в режиме обучения. Этот режим выявляет любые приложения, взаимодействующие с сетью, и выдает диалог с предупреждением сообщающем. Это все данные о приложение (т.е, в каком направлении запрашивается соединение, исходящие или входящие, через какой порт и по какому протоколу). Основываясь на предупреждении, пользователь выбирает соответствующие действия. Он может разрешить приложению выполнять любые действия либо запретить. Также можно создать правило, где все параметры задаются пользователем.

ЗАДАНИЕ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Задание:

1) Защитить машину брандмауэром и произвести сканирование.
2) Произвести настройку брандмауэра для устранения или скрытия найденных путем сканирования портов уязвимостей
3) Запретить доступ на виртуальной машине для HOST-компьютера и осуществить новое сканирование на уязвимости.
4) По завершении сканирования создать отчет и сравнить с сохраненными ранее.
5) Настроить правила для портов согласно Таблице №1.

Таблица 1 – Варианты заданий

№ варианта	Задание
1	Запретить исходящее соединение по протоколу TCP с адресом 192.168.120.1 через порт 110;
2	Запретить входящие данные по протоколу UDP от адреса 192.168.124.0 через порт 4000. При попытке установления связи через данный порт и адрес автоматически запустить антивирусную программу;
3	Разрешить входящие данные по протоколу IP, где протокол: 6 – Transmission Control Protocol, для IP-адресов следующего диапазона: 192.168.10.0-192.168.11.255;

№ варианта	Задание
4	Разрешить исходящее соединение для адреса 192.168.0.1
5	Запретить исходящее соединение с адресом 192.168.0.12 по протоколу TCP с портом 43;
6	Разрешить входящее соединение по протоколу IP с диапазоном адресов 192.168.0.1-192.168.3.255, где протокол: Internet Control Message Protocol-1;
7	Запретить входящие данные по протоколу UDP для диапазона адресов: 192.168.12.3-192.168.13.255;
8	Запретить исходящие данные по протоколу TCP по порту 145 для диапазона адресов: 192.168.12.3-192.168.13.255;
9	Разрешить исходящие данные для адреса 192.168.0.34 по протоколу TCP для порта 4000;
10	Запретить входящие данные по протоколу IP, где протокол: Internet Control Message Protocol-1, для диапазона адресов: 192.168.12.3-192.168.13.255.

Порядок выполнения работы:

1) Для того, чтобы просмотреть список глобальных правил, щелкните на панели инструментов кнопку Параметры, выберите вкладку Системные и щелкните Правила в группе Глобальные правила и доступ к rawsocket.

2) Для того, чтобы добавить новое правило, щелкните Добавить в окне диалога Глобальные правила. В окне редактирования правила укажите параметры.

3) Выберите событие для правила.

4) Выберите действие для правила.

5) Для защиты сессии NetBIOS необходимо добавить в область сетевого взаимодействия лишь те IP-адреса, которым вы полностью доверяете. Для этого перейдите в настройку системных параметров брандмауэра и нажмите на кнопку «Параметры» для настройки локальной сети. Нажав на кнопку «добавить», в обработку можно включить как отдельный IP-адрес, так и диапазон IP-адресов или отдельный домен

6) Выберите действия - соответствующие сообщения появятся в поле Описание правила. Если вы хотите, чтобы действием на событие стал запуск определенного приложения или команды, поставьте флажок в соответствующем поле и укажите приложение или команду, нажав на подчеркнутое значение в поле Описание правила.

7) Убедитесь, что в поле Описание правила не осталось неопределенных параметров. Outpost Firewall Pro автоматически сгенерирует Имя правила на основе заданных параметров. Щелкните OK, чтобы сохранить правило. Правило отобразится в списке.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Шувалов В.П., Величко В.В., Субботин Е.А., Ярославцев А.Ф. Телекоммуникационные системы и сети. Том 3. Мультисервисные сети (2005)

2) Петраков А.В. Основы практической защиты информации. 2-е изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.

3) Цифровые и аналоговые системы передачи: Учебник для вузов/ В.И.Иванов, В.Н.Гордиенко, Г.Н.Попов и др.; Под ред. В.И.Иванова. – 2-е изд. – М.: Горячая линия – Телеком, 2003.–232 с.

4) Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов. - СПб.: БХВ-Петербург, 2010. - 400 с.

5) Башарин Г.П. Лекции по математической теории телетрафика: Учеб. пособие. Изд. 3-е, испр. и доп. - М.: РУДН, 2009.-342 с.

6) Буч Г. Объектно-ориентированный анализ и проектирование. – М.: Вильямс, 2008.

7) Леоненков А.В. Самоучитель языка UML. – СПб.: БХВ-Петербург, 2004.

8) Розенберг Д., Скотт К. Применение объектного моделирования с использованием UML и анализ прецедентов. – М.: ДМК Пресс, 2002.

9) А.В. Росляков. Виртуальные частные сети. Основы построения и применения. - М.: Эко-Трендз, 2006. - 242 с.