**Внимание!** Срок выполнения заданий – **до 11:15 (мск) 19.12.2019г**. Ответы, присланные позднее, рассматриваться не будут!

Для выполнения практических заданий необходимо предварительно подготовить тестовый стенд из двух виртуальных машин или физических компьютеров и обеспечить между ними сетевое взаимодействие. Виртуальные машины можно создать и настроить в структуре ESXi-сервера или в VMware Workstation самостоятельно или развернуть их из прилагаемых образов.



 на компьютере VM1 установлена ОС Windows 7 SP1 x64 с параметрами сетевого соединения: IP-адрес – **192.168.101.11**, маска – **255.255.255.0**. Отключен протокол IPv6. Реквизиты учетной записи с правами локального администратора: логин – **adminsns**, пароль – **P@ssw0rd**. Проведена автономная установка клиента Secret Net Studio 8.5 без компонента "Доверенная среда";

 на компьютере VM2 установлена ОС Windows 7 SP1 x64 с параметрами сетевого соединения: IP-адрес – **192.168.101.22**, маска – **255.255.255.0**. Отключен протокол IPv6. Реквизиты учетной записи с правами локального администратора: логин – **Администратор**, пароль – **P@ssw0rd**. Установлены утилиты Wireshark, Ettercap и nmap.

**Внимание!** Если виртуальные машины были развернуты из прилагаемых образов, то перед началом выполнения заданий следует:

* в аппаратную конфигурацию виртуальных машин (выключенных) добавить по одному сетевому адаптеру (E1000) и подключить их к одному и тому же виртуальному коммутатору (любому выбранному или созданному);
* включить виртуальные машины и настроить параметры сетевых соединений согласно описанию конфигурации виртуальных машин (см. выше);
* с помощью утилиты **ping** убедиться, что между ВМ VM1 и VM2 есть сетевое взаимодействие. Если это не так, убедитесь, что на всех ВМ отключен брандмауэр Windows.

Подробное описание виртуальных машин см. в файле **"IB\_school\_stand.doc"**.

## Практическое задание №1. Настроить правила разграничения доступа в межсетевом экране Secret Net Studio и проверить его работу

**1.** На компьютере VM1 с установленным клиентом Secret Net Studio сделайте следующее:

 установите разрешение подключения к данному компьютеру через удаленный рабочий стол (RDP);

 создайте на локальном диске папку с произвольным наименованием, например, "user\_files" и в ОС Windows настройте для нее общий доступ с максимальными разрешениями;

 с компьютера VM2 убедитесь, что подключение к компьютеру VM1 через удаленный рабочий стол и обращение к общей папке ("user\_files") возможны.

**2.** Добавьте запрещающие правила:

 правило доступа, запрещающее доступ к VM1 (192.168.101.11) по протоколу RDP всем портам для всех пользователей и IP-адресов;

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Пользователь | Источник | Протокол/порт | Получатель | Протокол/порт | Действие |
| everyone | any | any/any | 192.168.101.11 | TCP, UDP/3389 | deny |

 активируйте механизм ICMP-защиты с настройками по умолчанию.

**3.** Сохраните сделанные настройки. С компьютера VM2 убедитесь, что компьютер VM1 недоступен через утилиту ping и удаленный рабочий стол.

**4.** Добавьте следующие правила:

 системное правило, разрешающие доступ к VM1 (192.168.101.11) по протоколу ICMP для всех пользователей c IP-адреса 192.168.101.22 (с VM2);

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Пользователь | Источник | Протокол/порт | Получатель | Протокол/порт | Действие |
| everyone | 192.168.101.22 | any/any | 192.168.101.11 | ICMP/any | allow |

 прикладное правило, запрещающее доступ к общедоступной папке "user\_files" на ВМ VM1 (192.168.101.11) с любого компьютера. При этом активируйте опцию добавления соответствующего правила доступа, разрешающего прохождение пакетов по протоколу TCP на порт 445 (и/или 139);

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Пользователь | Источник | Протокол/Порт | Получатель | Протокол/Порт | Действие |
| everyone | any | any/any | 192.168.101.11 | SMB/any | deny |

 c помощью расположенных под таблицей "Правила доступа" кнопок "Вниз"  и "Вверх"  установите приоритет всех добавленных разрешающих правил выше, чем всех запрещающих (переместите запрещающие правила в нижнюю часть таблицы, после разрешающих). Примените сделанные настройки.

**5.** С компьютера VM2 убедитесь, что компьютер VM1 снова стал доступен через утилиту ping, а обращение к общей папке "user\_files" блокируется.

**6.** Для выполнения следующего задания выполните одно из следующих действий:

 отключите все добавленные в настройки межсетевого экрана запрещающие правила и сохраните сделанные изменения;

 на вкладке "Состояние" выключите компонент защиты "Персональный межсетевой экран" и перезагрузите компьютер VM1.

## Практическое задание №2. Настроить компонент СОВ в Secret Net Studio и проверить его работу

**1.** Проведите настройку СОВ на клиенте SNS, установленном на VM1, применив следующие политики:

 "Включить детекторы атак" – установите флажок;

• "Блокировка атакующего хоста…" – оставьте отмеченным, "Время блокировки" – 1 минута;

• "Использовать черный список IP-адресов" – оставьте отмеченным (параметр по умолчанию активен для всех детекторов). В этом случае будут заблокированы вредоносные IP-адреса из базы опасных веб-ресурсов Kaspersky;

• в группе "Детекторы" установите отметку в поле "Сканирование портов". В параметрах "Период обнаружения" и "Максимальное количество обращений к портам" оставьте значения по умолчанию;

• в разделе "Регистрация событий / Обнаружение вторжений" оставьте активными следующие события: "Сработал детектор вторжений", "СОВ заблокировал удаленный узел" и "СОВ разблокировал удаленный узел";

• сохраните сделанные настройки.

2. Перейдите в консоль ВМ VM2 и проведите сканирование портов компьютера VM1 с помощью команды: **nmap -T5 -PN 192.168.101.11**.

С помощью утилиты **ping** проверьте доступность компьютера VM1 (192.168.101.11) и убедитесь, что эхо-ответы не приходят.

3. Просмотрите записи журнала тревог, указав тип событий "Аудит отказов" или "Ошибка".

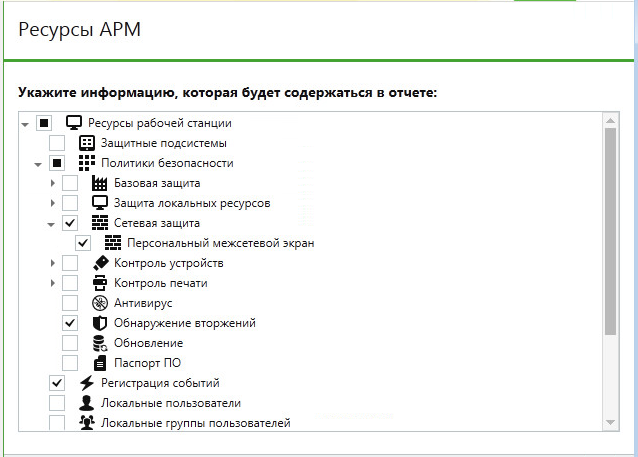
## Практическое задание №3. Подготовить отчет о сделанных на клиенте Secret Net Studio настройках и добавить свои анкетные данные

**1.** Восстановите сделанные в задании 1 настройки межсетевого экрана, выполнив одно из следующих действий:

 включите все добавленные ранее в настройки межсетевого экрана правила и сохраните сделанные изменения;

 на вкладке "Состояние" включите компонент защиты "Персональный межсетевой экран" и перезагрузите компьютер VM1.

**2.** Сформируйте отчет по результатам сделанных настроек, установив параметры, как показано на рисунке.



**3.** В файл отчета добавьте свои анкетные данные, заполнив следующие поля в "шапке":

 "Рабочее место" – наименование учебного заведения или наименование организации + город;

 "Номер системного блока" – курс или оставьте пустым, если вы не студент;

 "Тип компьютера" – специальность/направление обучения или должность;

 "Ответственный работник" – Фамилия, Имя, Отчество;

 "Наименование СУБД" – адрес электронной почты.