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-41-20 | | | | | | | |
| ФИО: | Ахтямов В.И. | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2023г. | |
| Оценка: |  | | | | | | | |

**Результаты выполнения лабораторной работы**

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

Выбор был в ользу сетей NAT, поскольку благодаря этому виду подключения, все машины, подключенные к одной сети могут получить доступ друг к другу, а если выбрать подключение через NAT, то есть доступ в интернет, но нет связи между машинами.

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

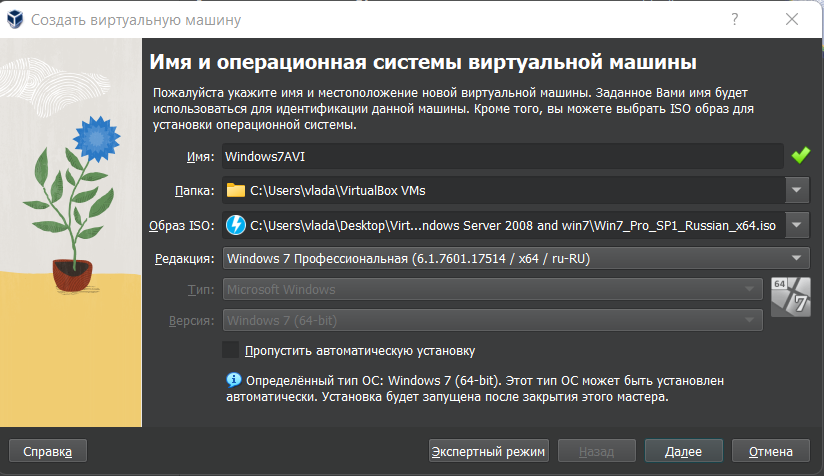
- VirtualBox с видимым наименованием созданных Вами виртуальных машин

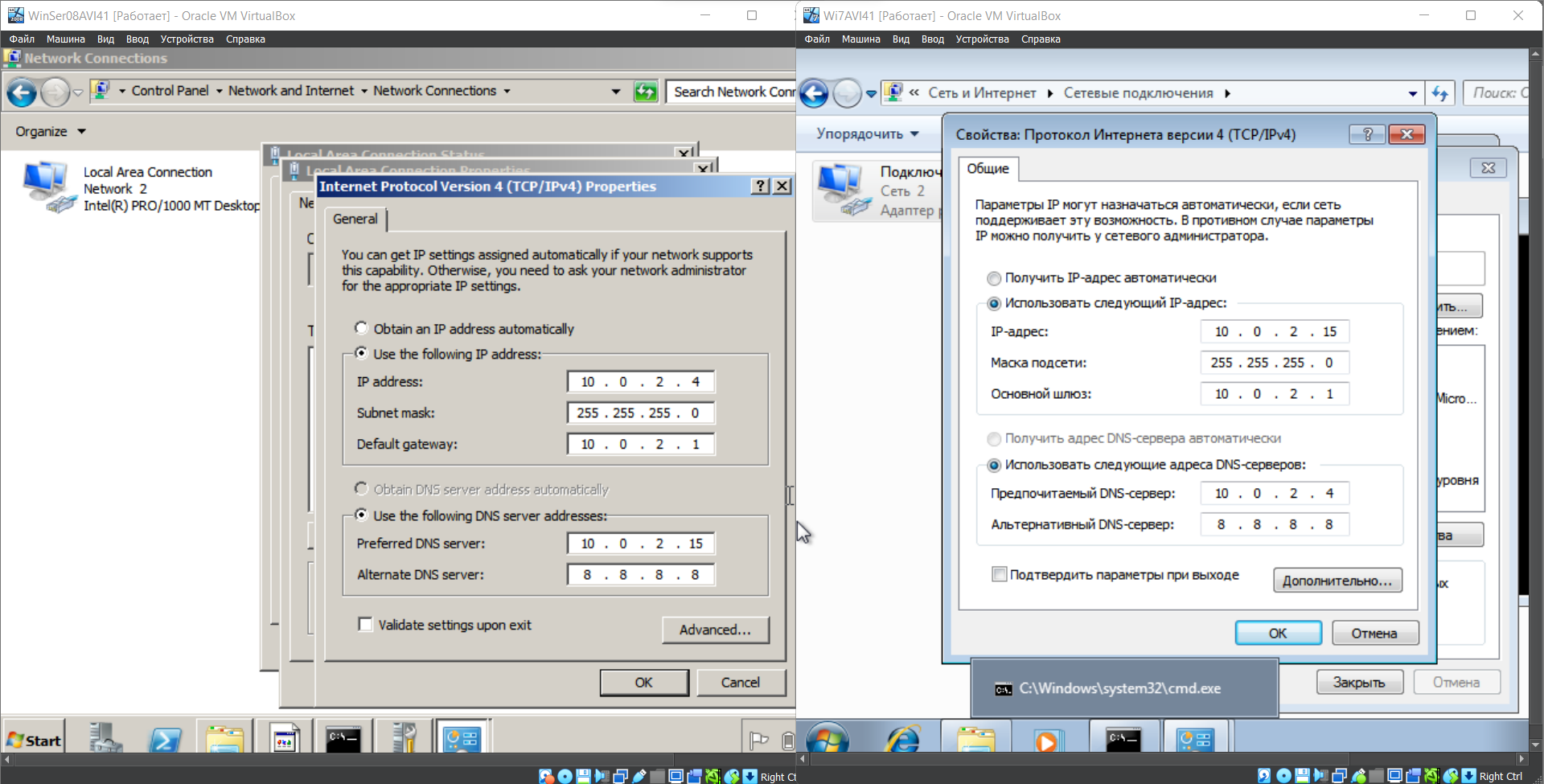
- VirtualBox с открытым в Windows 7 окном «Свойства: Протокол Интернета версии 4 (TCP/IPv4)», в котором видны прописанные статические параметры сети

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

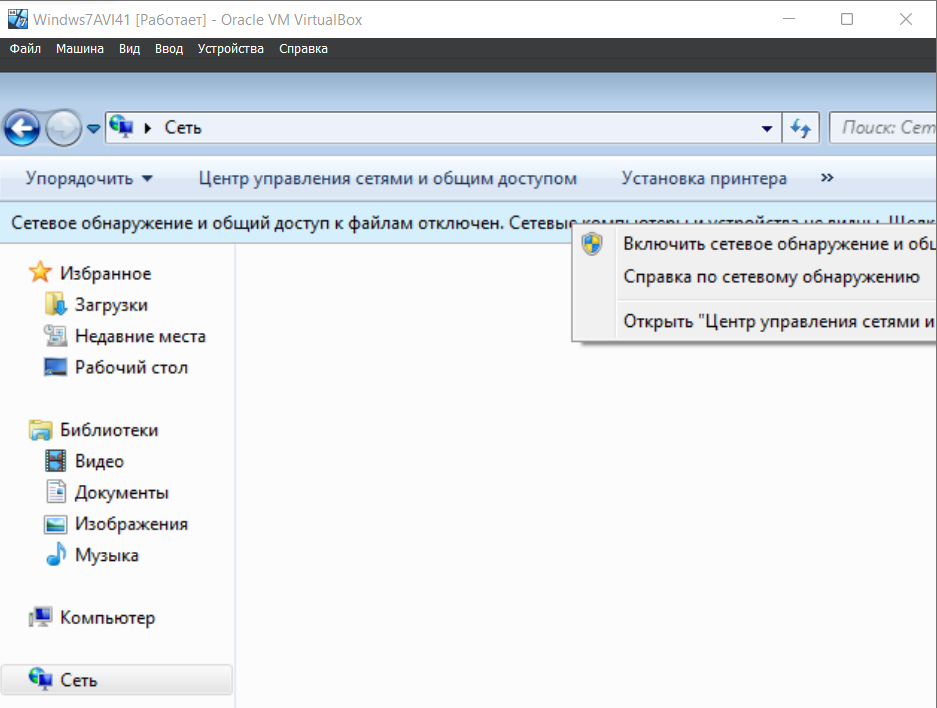
|  |
| --- |
| Скриншот № 1 |
| Этот шаг, для того чтобы просто поменять ip адрес машин, который виден в сети – это было делать не обязательно, просто чтобы ip совпадали с лабником  В windows 7 мы устанавливаем предпочитаемый dns сервер = ip server2008, поскольку это позволит win7 найти контроллеры домена и другие службы AD. То есть, чтобы в будущем мы могли с win7 зайти под другим пользователем, которого зарегистрировали в AD – user1  Указание IP-адреса сервера Windows Server 2008 в качестве предпочитаемого DNS-сервера на компьютере, который вы хотите добавить в домен, позволяет компьютеру правильно находить контроллеры домена и другие службы AD, и таким образом, успешно присоединиться к домену.  Контроллеры домена - это серверы, которые управляют и поддерживают доменную среду в сети Active Directory (AD) на сервере Windows. Они выполняют ряд важных функций, таких как аутентификация пользователей, авторизация доступа к ресурсам, управление политиками безопасности, репликация информации о домене между различными контроллерами домена и другие задачи, связанные с управлением доменом.  Контроллеры домена хранят информацию о пользователях, группах, компьютерах и других объектах, зарегистрированных в домене, в своей базе данных. |

Обязательно при создании – выбираем профессиональную windows 7 – иначе не удастся добавить с win7 в домен под созданным пользователем user1

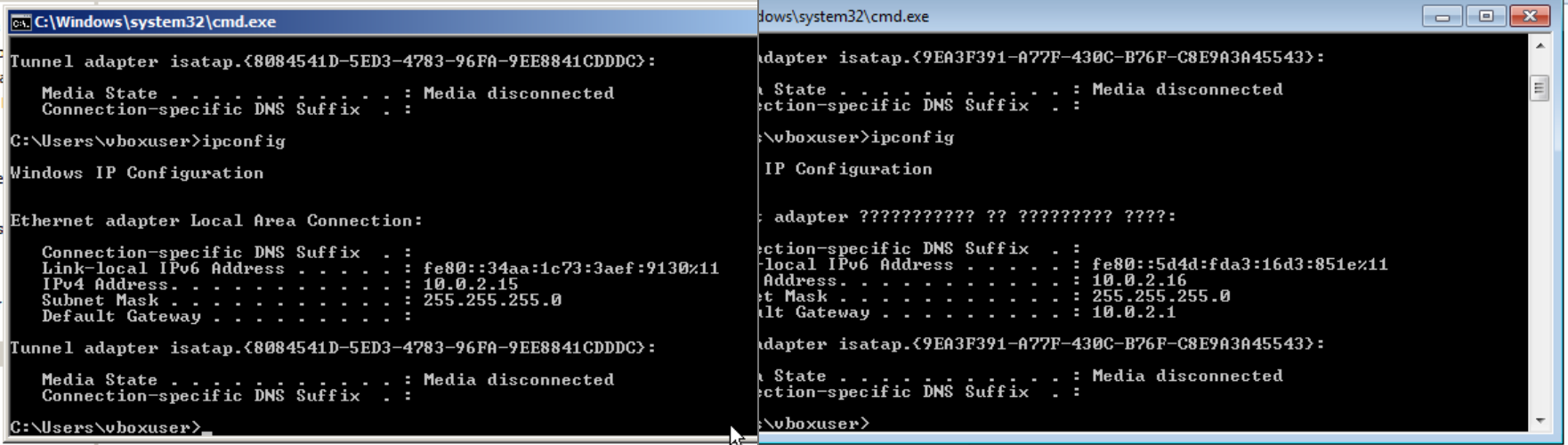




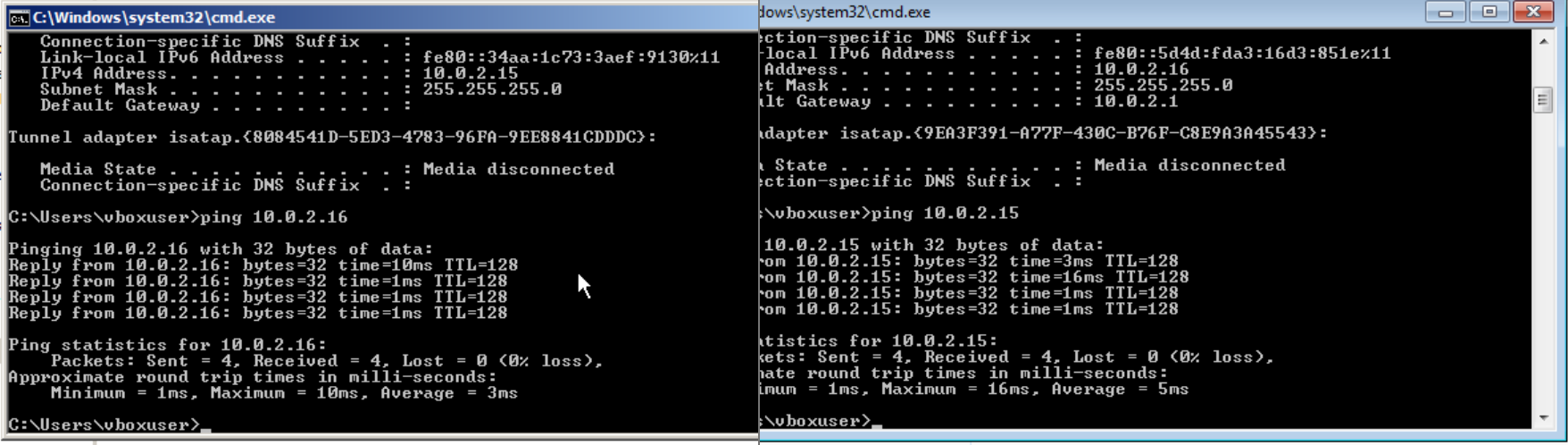
Далее было необходимо включить сетевые подключения



Отлично новые ip адреса были успешно установлены

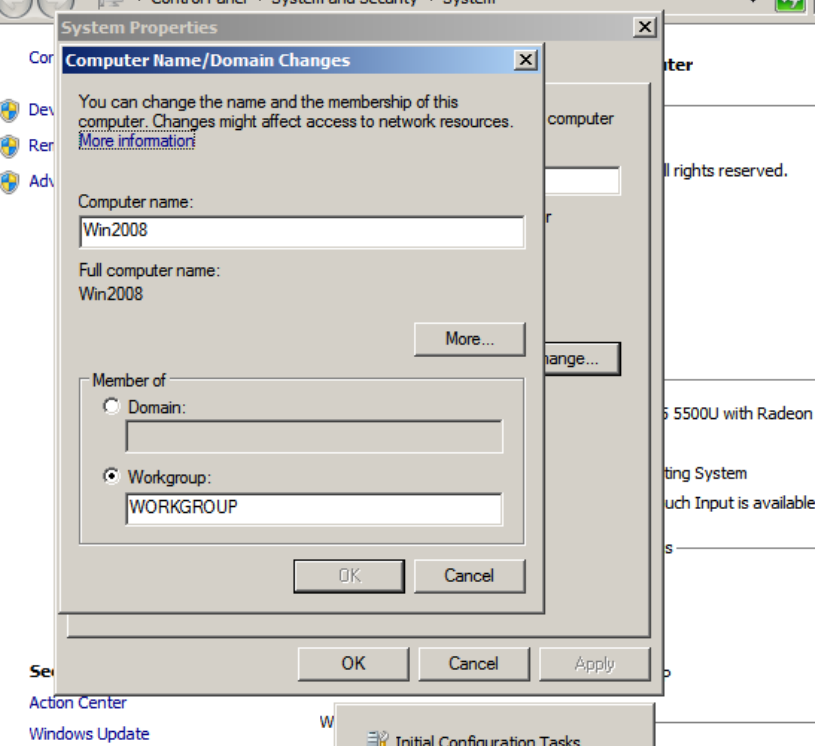


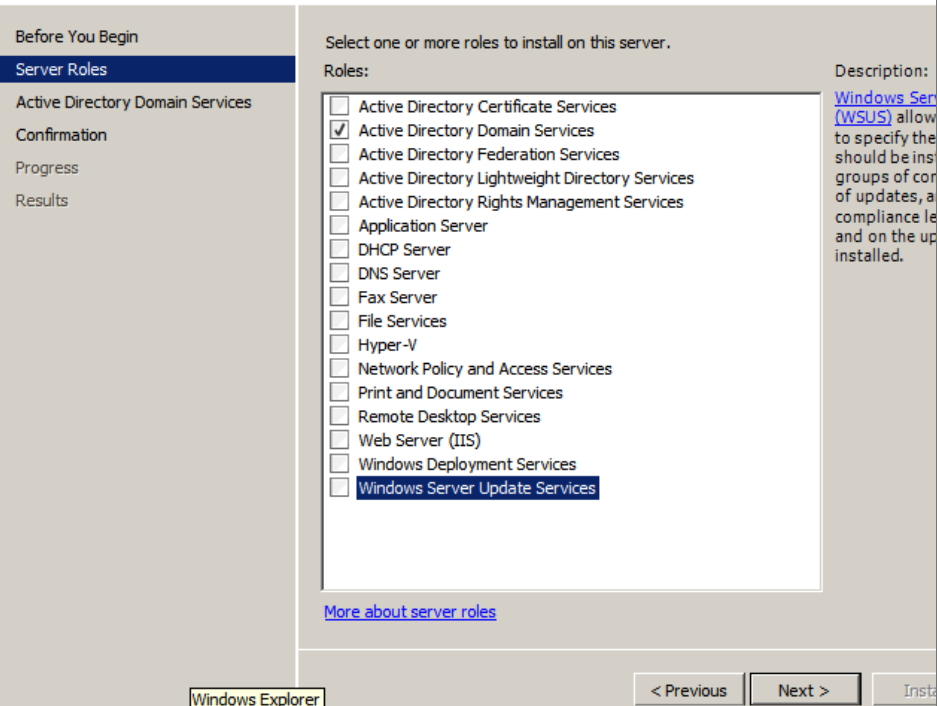
И после включения сети компьютеры пингуются



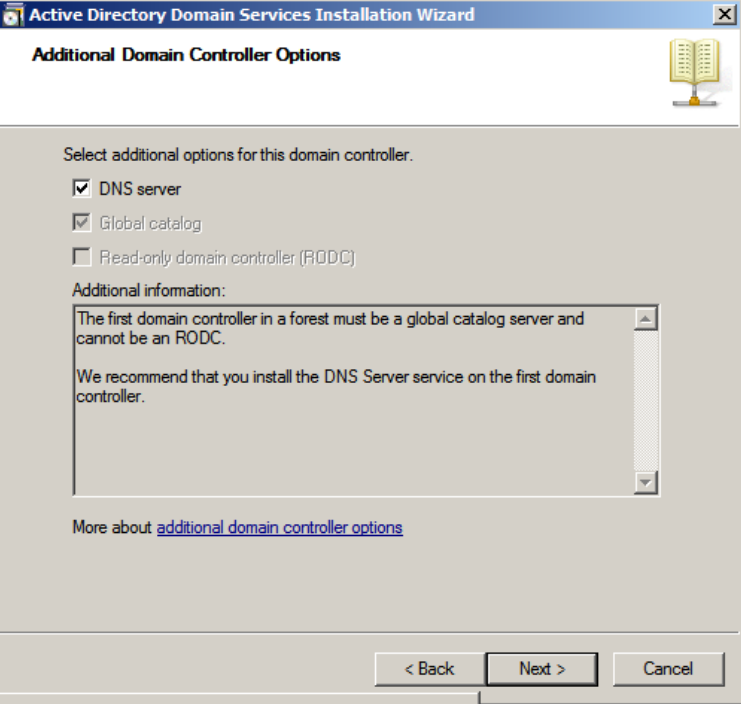
2. Результаты создания доменного пользователя на Windows 7.

|  |
| --- |
| Скриншот № 2 |



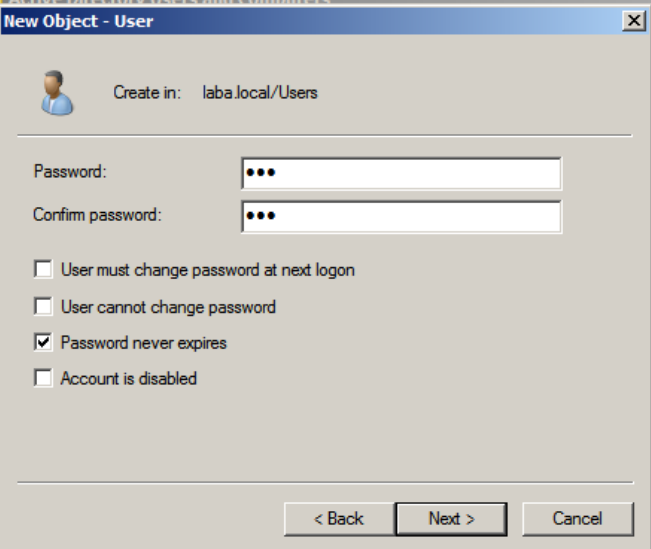


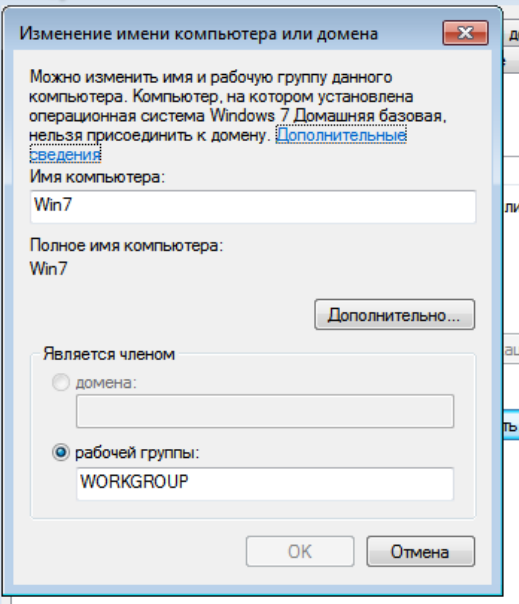
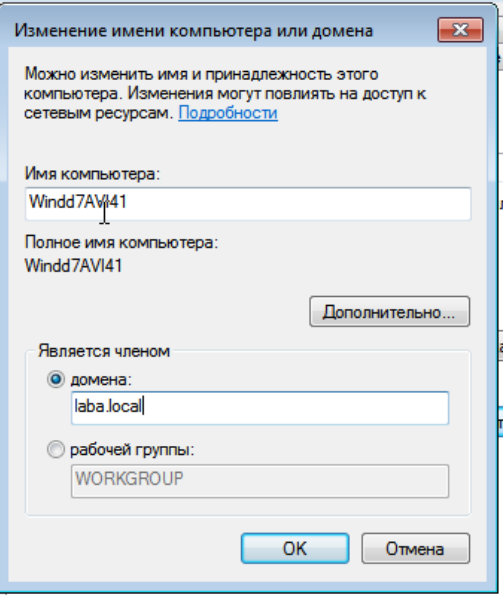
В терминологии Active Directory (AD) в Windows Server, создание нового домена в новом лесе означает создание нового домена и отдельной сети доверия, которая не имеет связи с существующими доменами или лесами AD. Лес - это логическая структура, которая объединяет один или несколько доменов в единое доверительное отношение.

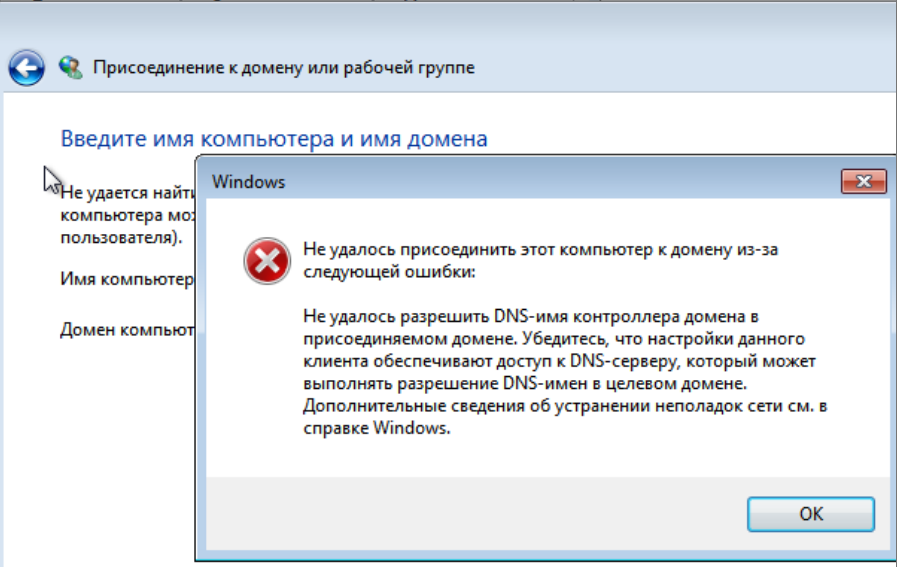


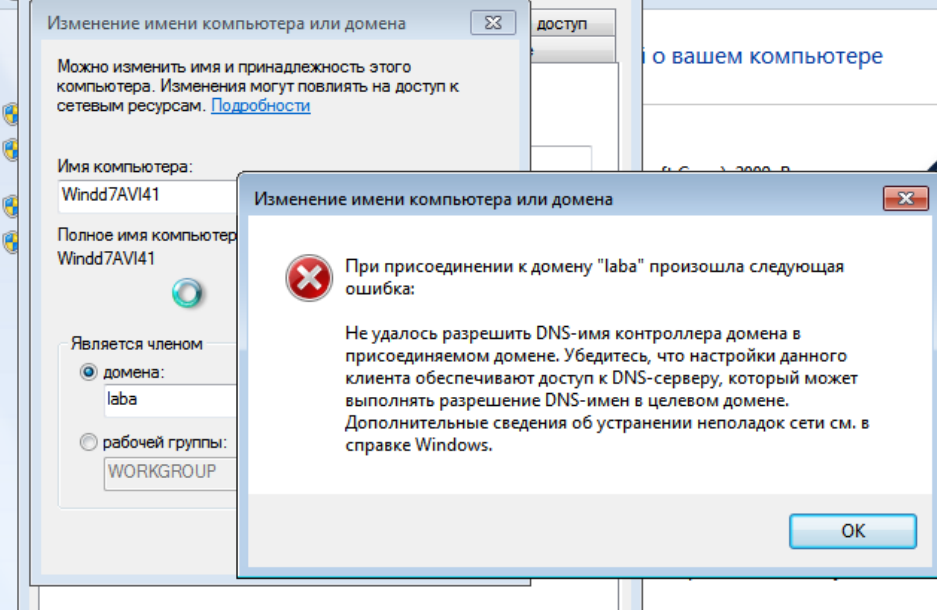


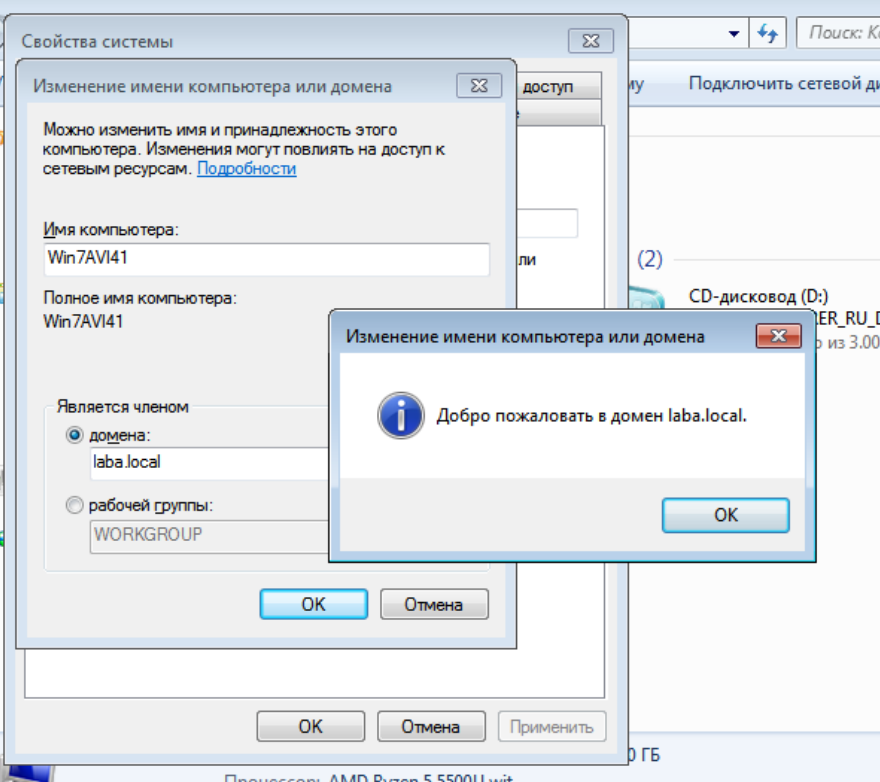
Далее добавляем нового пользователя, принадлежащего к этому домену









3. Окно входа в Windows 7 под доменным пользователем

|  |
| --- |
| Скриншот № 3  Чтобы на Windows 7 зайти под пользователем в домене. Для этого на стартовом окне после ввода клавиш Ctrl+Alt+Delete  Но не получается нажать эти клавиши, для этого есть: |
|  |

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

|  |
| --- |
| Скриншот № 4 |
|  |
|  |
|  |
|  |
| Далее  HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters  Выставить 0 для:  EnableSecuritySignature  RequireSecuritySignature  Для чего – я написал ниже  Делаем мы это – потому что responder не сможет перехватить хеш |

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

Подписывание SMB (также известное как сигнатуры безопасности) — это механизм безопасности в протоколе SMB. Подписывание SMB означает, что каждое сообщение SMB содержит сигнатуру, созданную с помощью ключа сеанса. Клиент помещает хэш всего сообщения в поле сигнатуры заголовка SMB.

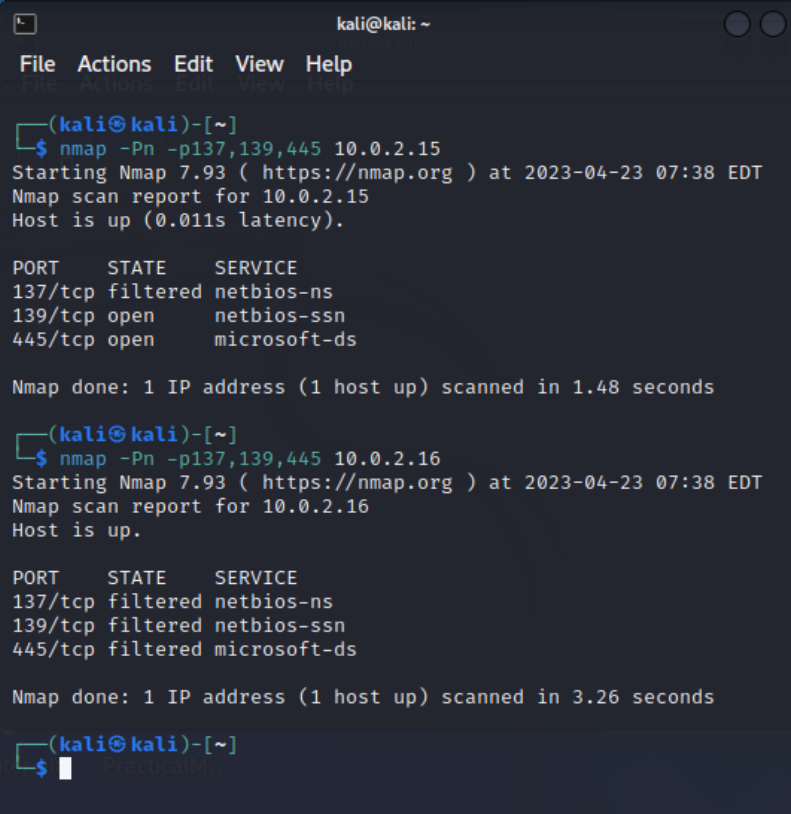
Отключая SMB мы уменьшаем уровень защищенности.

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

nmap -Pn -p137,139,445 10.2.0.15 -

nmap -Pn -p137,139,445 10.2.0.16

Данные команды используются для проверки существования в сети соединения по протоколу SMB, которое мы настраивали ранее



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

Responder это инструмент для выполнения атаки человек-посередине в отношении методов аутентификации в Windows. Эта программа включает в себя травитель LLMNR, NBT-NS и MDNS благодаря которому перенаправляется трафик с запросами и хешами аутентификации. Также в программу встроены жульнические серверы аутентификации HTTP/SMB/MSSQL/FTP/LDAP, которые поддерживают такие методы аутентификации как NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP и базовую HTTP аутентификацию, для которых Responder выполняет роль ретранслятора.

То есть пытается уловить хеши паролей при действиях пользователя

|  |
| --- |
| Скриншот № 5  Чтобы получить хеш, нужно было еще изменить файл responder.conf – заменить у smd и http с off на on |

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

|  |
| --- |
| Скриншот № 6  Далее вместо скачивания mgw, перейдем в папку и запустим multirelay.py    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)  И получаем результат |

9. Ответ на вопросы лабораторной работы:

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

Mimikatz – это приложение, которое позволяет осуществлять атаки на учетные данные аутентификации.

В данной лабораторной работе мы получили удаленный доступ к серверу. Далее мы скачиваем приложение mimikatz.exe на него. А далее с помощью него получаем учетные данные хостов.

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

|  |
| --- |
| Скриншот № 7  Теперь в условиях задания большая путаница - теперь почему-то утверждается, что win7 под 10.0.2.15, хотя он по 10.0.2.16  Если закинуть Мимикатз на server2008, то он там не выполняется:  А на win7 вообще нет возможности перекинуть, так как не выходить установить связь С2    И я решил попробовать запустить mimicatz на server2008 – так как только туда его удалось закинуть – но там проблемы с привеллегиями |

11. Индивидуальные выводы по лабораторной работе.

В данной лабораторной работе были продемонстрирована атака на кражу учетных данных пользователя.

Я ознакомился с возможностями таких утилит, как Responder – благодаря которому был перехвачен хеш пароля, и с помощью MultiRelay – установление удаленного подключения к серверу.

Далее я изучил возможность такого средства, как mimikatz, котрый при запуске на удаленном сервере с флагами privilege::debug sekurlsa::logonpasswords позволил перехватить пароли всех пользователей в домене.

Опыт полученный с этой лабораторной работы был очень полезен для меня.

В итоге инструменты:

Responder – чтобы перехватить хеши пароля

Multirelay – чтобы установить связь С2 с кали на сервер или win7

Mimicatz – чтобы перехватить запрсы 7ки к серверу и украсть пароли