**Модуль 26.7 Атаки на Active Directory**

[Course | SkillFactory](https://apps.skillfactory.ru/learning/course/course-v1:SKILLFACTORY+hack_pentest+2020/block-v1:SKILLFACTORY+hack_pentest+2020+type@sequential+block@b38b721359a54dd3a18fb2f024b26c86/block-v1:SKILLFACTORY+hack_pentest+2020+type@vertical+block@1cd329234245485bb89787e38dc6c9c5)

Лабораторная работа.

Используя ранее поднятый домен вашей тестовой лаборатории (см.[SF+H\_25.7 - Google Документы](https://docs.google.com/document/d/1TmxJsTQKUU3s9smqsECy1Ef3PL2Yvtw0-Lc4R66pQdM/edit)):

0

Введите ещё одну машину в домен.

В отчёт включить скриншот «Сведения о компьютере», чтобы был виден домен.

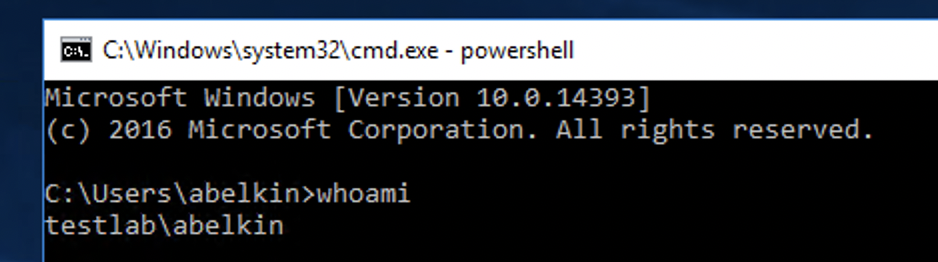
1

Брутфорс УЗ с помощью утилиты *hydra* и *Kali Linux*.

2

Соберите информацию о домене (максимально, сколько найдёте).

В отчёт включить скриншоты данных (например, вывод любой использованной команды), которые смогли получить.



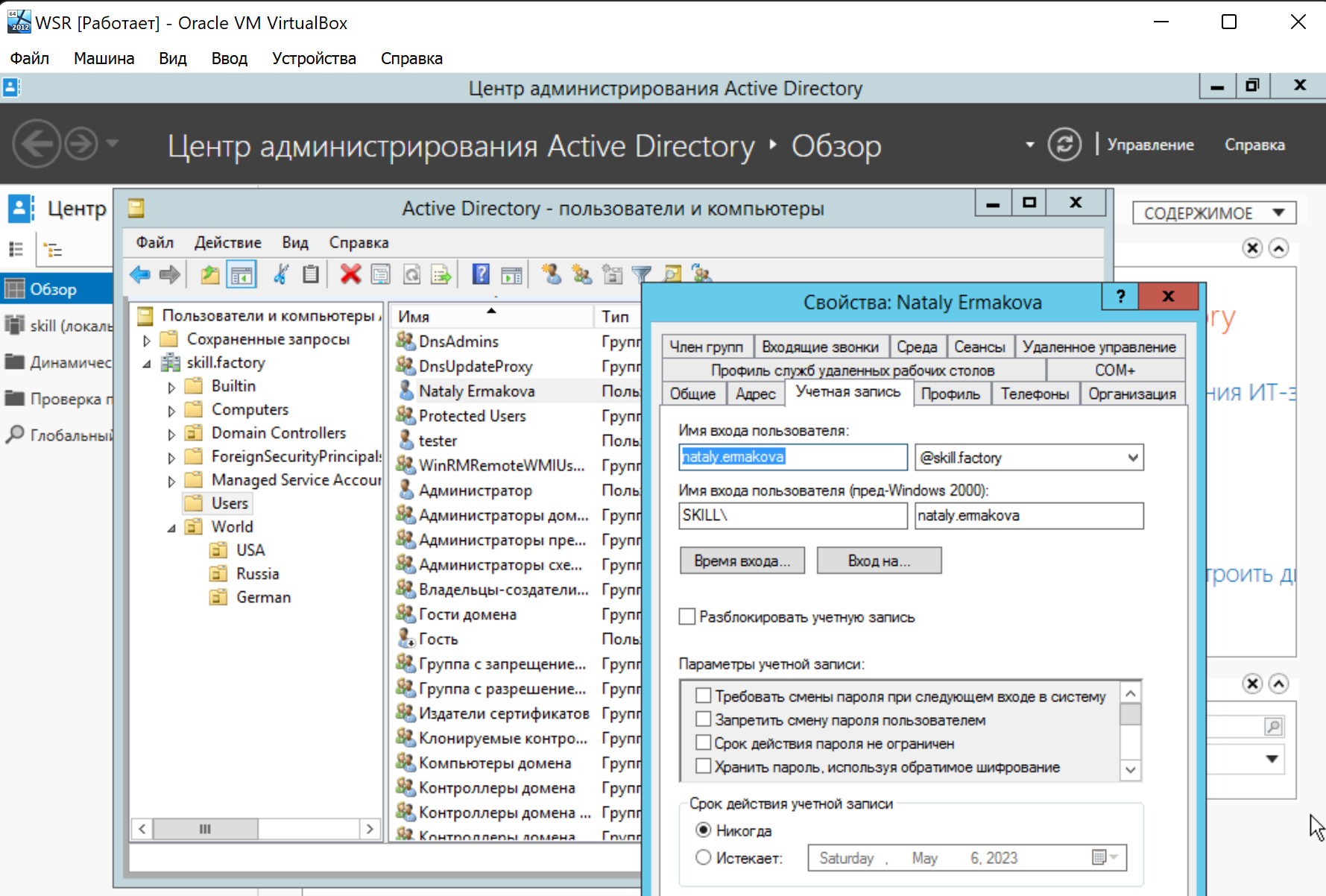
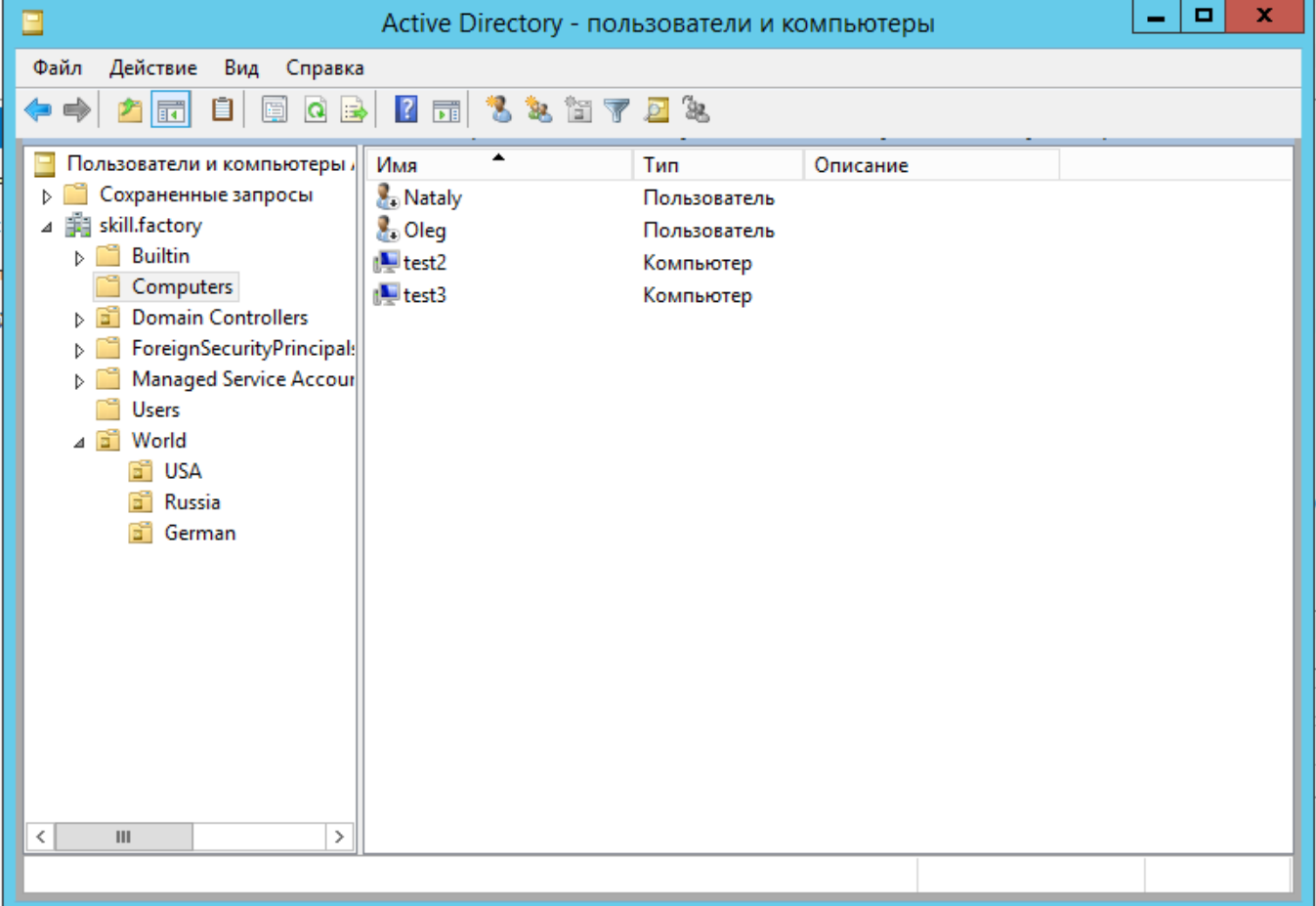
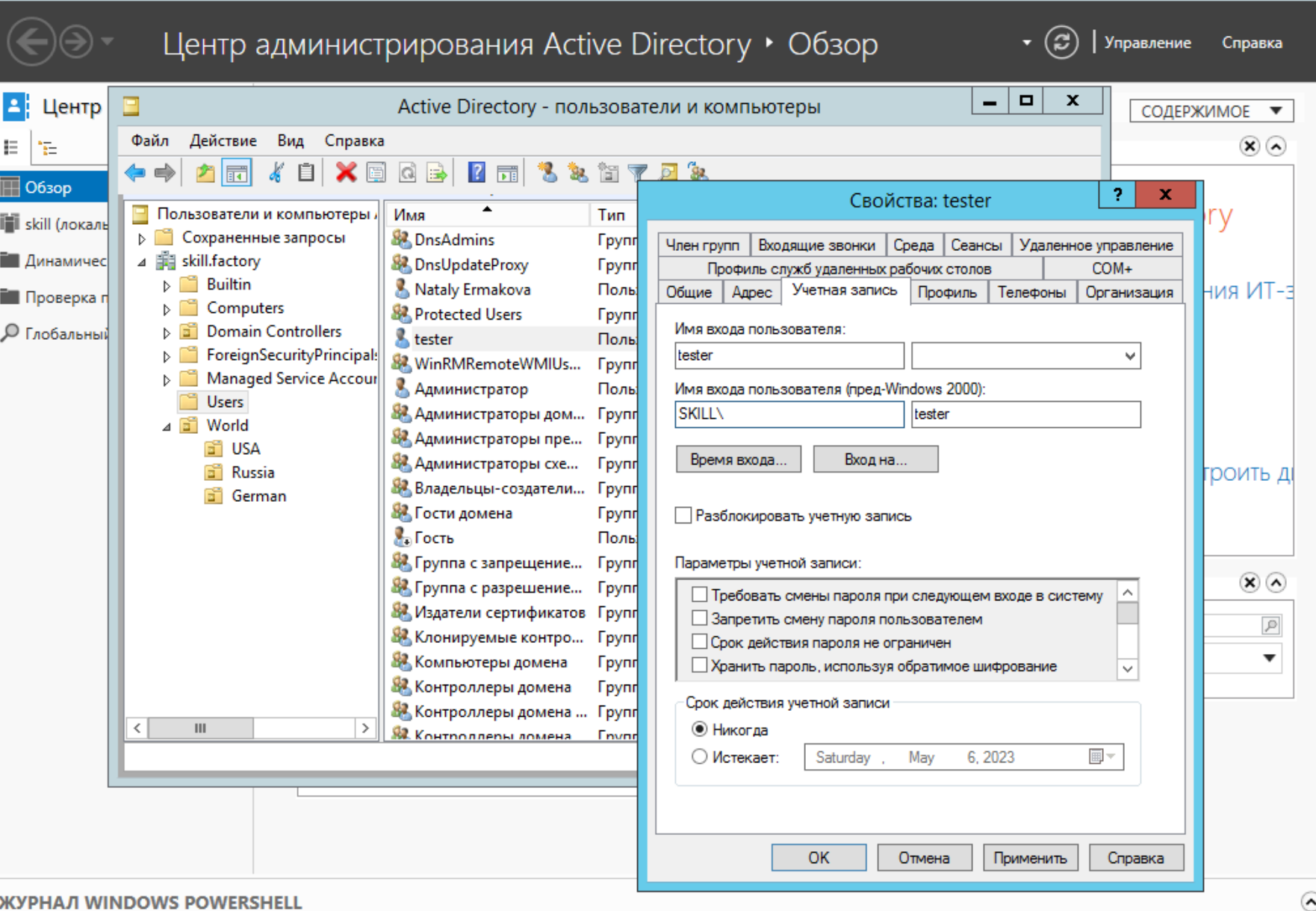
3

Используя *latmov*, попробуйте подключиться к любой другой машине в домене (не ограничиваем в использовании инструментов/техник/тактик).

В отчёт включите скриншот подключения к другой машине.

**Решение.**

1. Основываясь на предыдущей лабораторной работе (см.[SF+H\_25.7 - Google Документы](https://docs.google.com/document/d/1TmxJsTQKUU3s9smqsECy1Ef3PL2Yvtw0-Lc4R66pQdM/edit)), ввела еще несколько машин в домен.

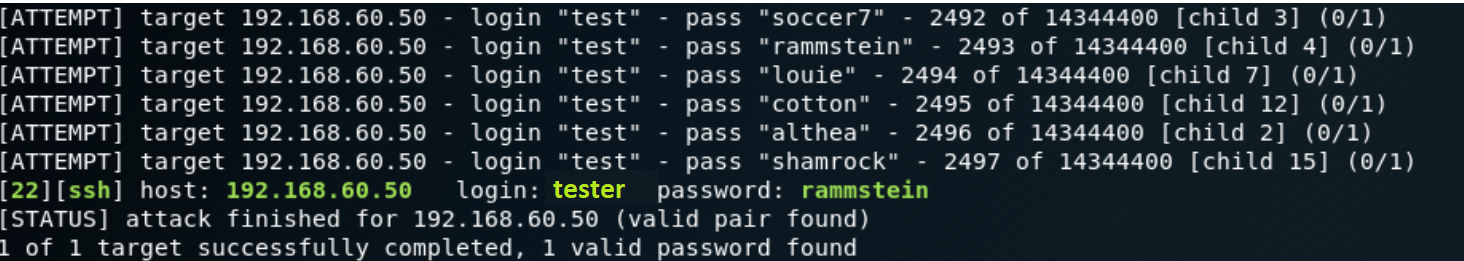


1. Брутфорс УЗ с помощью утилиты *hydra* и *Kali Linux*.

Скачиваем лист с разными паролями, например, отсюда - <https://raw.githubusercontent.com/berandal666/Passwords/master/10_million_password_list_top_100.txt>

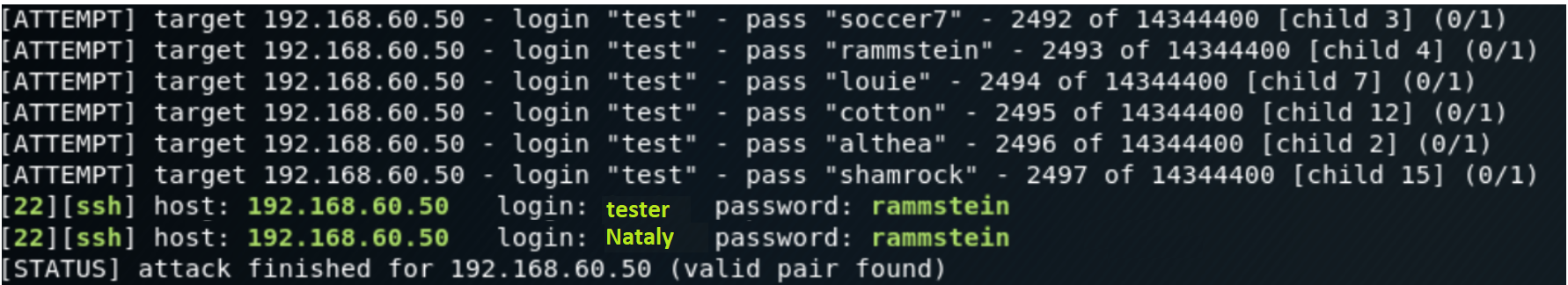
Для подбора пароля используя Hydra выполним команду:

hydra -V -f -t 4 -l test -P /root/wordlist ssh://192.168.60.50

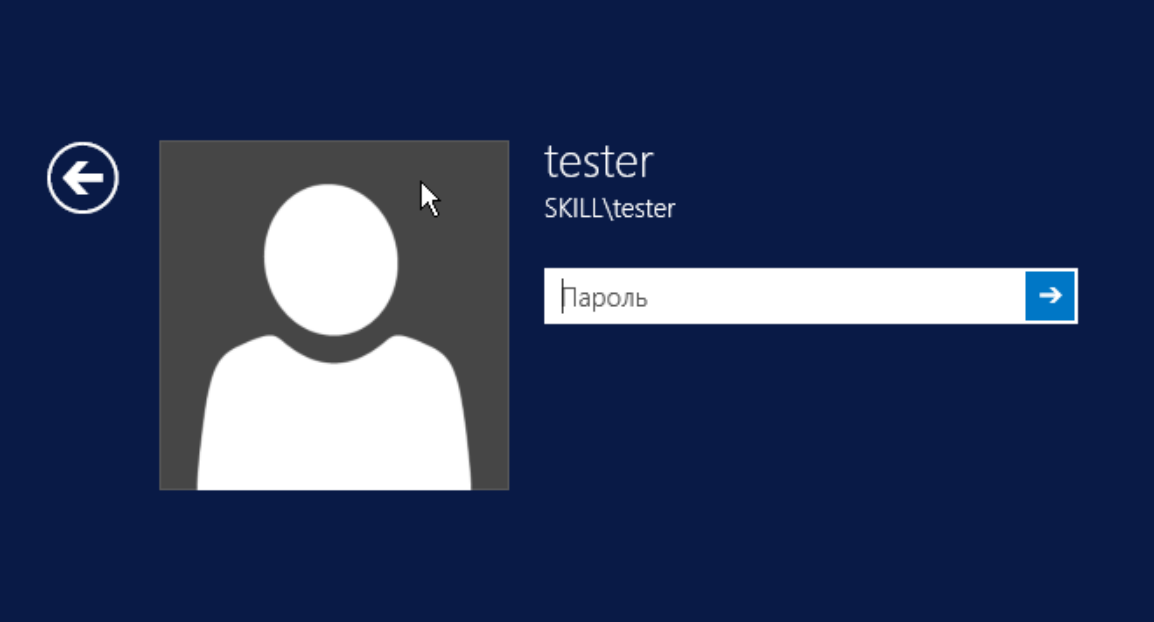


Пройдемся по домену и составим файл с пользователями домена. Проверим какие пользователи имеют одни и те же пароли.

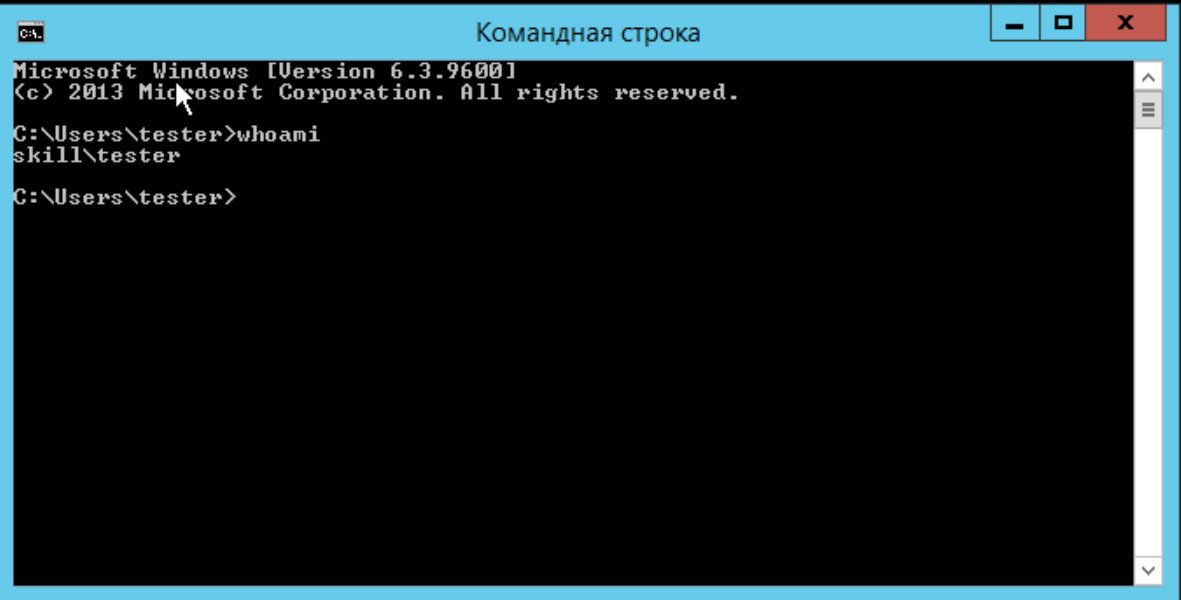
hydra -L /root/username -P /root/wordlist.txt 192.168.60.50 smb или hydra -p "пароль" -L users.txt smb://192.168.60.50 -m 'домен'



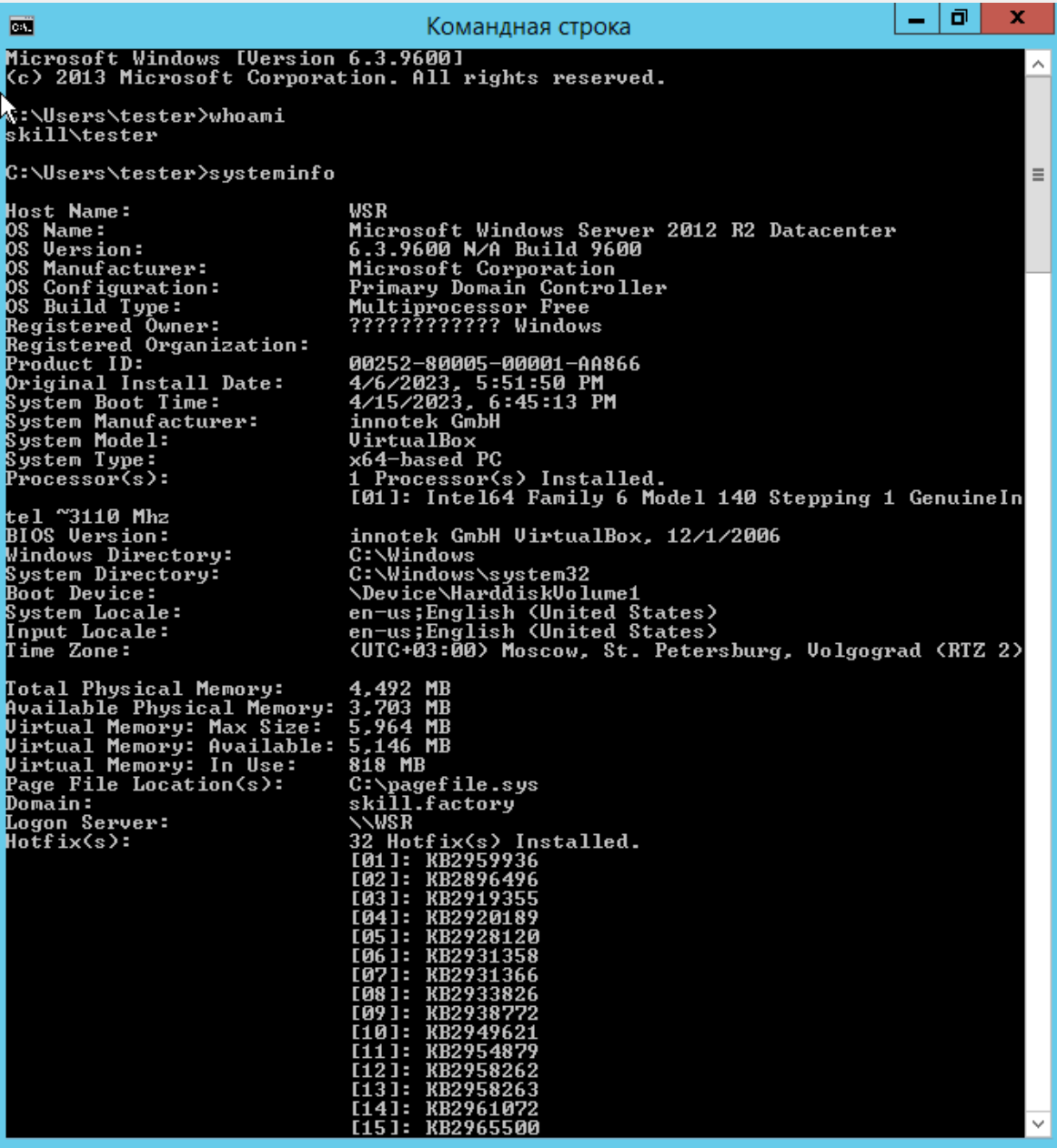
Зайдем на машину tester.



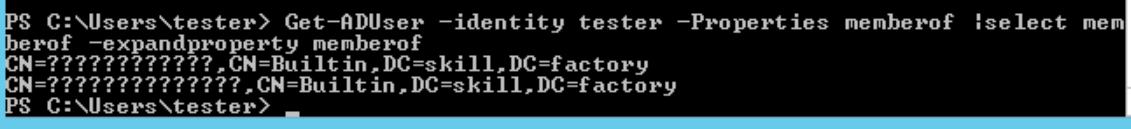
В cmd пишем команду whoami.



Напишем команду systeminfo, проверим.



Посмотрим какими правами обладает пользователь, используя команду в Powershell Get-ADUser -identity tester -Properties memberof| select memberof -expandproperty memberof



1. Используя *latmov*, попробуйте подключиться к любой другой машине в домене.

С помощью команды

Get-ADcomputer -Filter \* -Properties \* | FT name, ipv4Address

можно вывести все ip-адреса одного домена и через RDP зайти на один из них.