GOAD — лаборатория для практики взлома Active Directory

spy-soft.net/goad-lab-practice-active-directory-hacking

5 сентября 2024 г.

Мы уже рассказывали о безопасной среде для оттачивания навыков взлома Active Directory, которая называется Vulnerable-AD. Сегодня я хочу рассказать еще об одном проекте — GOAD (Game of Active Directory) — это стенд, специально созданный для тестирования на проникновение в среде Active Directory. GOAD предоставляет готовую к использованию, намеренно уязвимую инфраструктуру, идеальную для практики различных техник атак.

Еще по теме: Взлом и защита Active Directory

GOAD — стенд для практики взлома Active Directory

Это отличный проект, который позволяет пентестерам практиковать различные техники атак в уязвимой среде Active Directory.

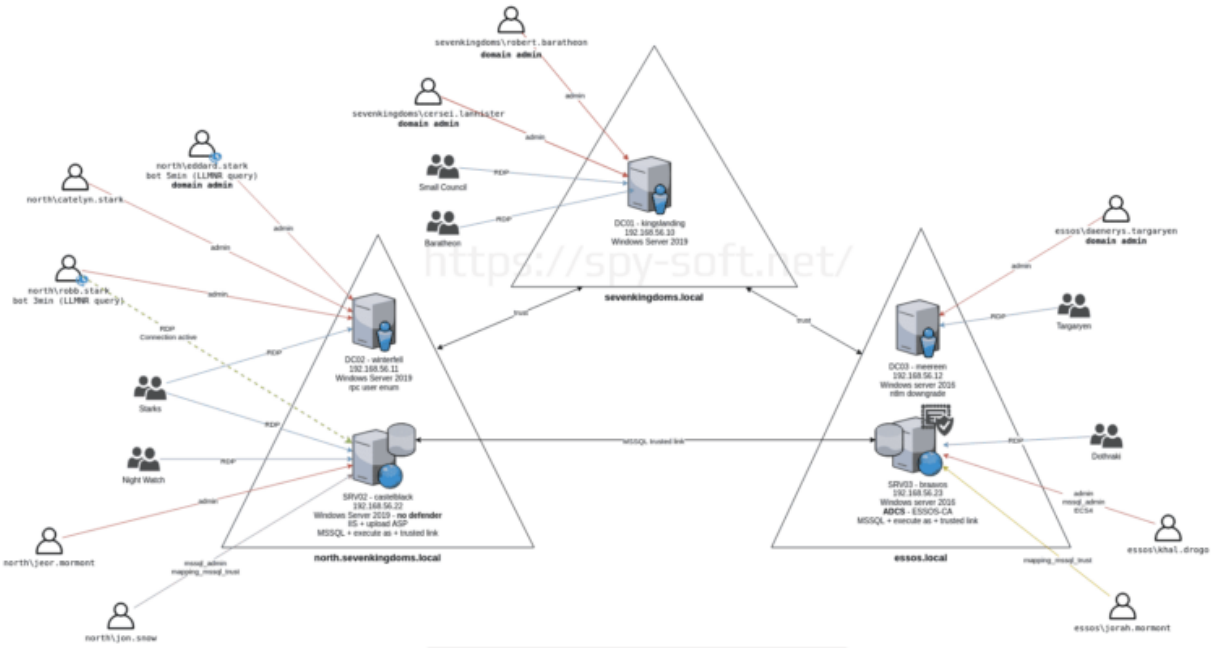
> Лаборатория крайне уязвима. Не используйте ее конфигурацию для создания реальных сред и не разворачивайте ее в интернете без изоляции.

В лаборатории используются бесплатные виртуальные машины Windows с ограниченным сроком действия 180 дней. По истечении этого срока вам нужно будет либо ввести лицензию на каждом сервере, либо заново установить лабораторию.

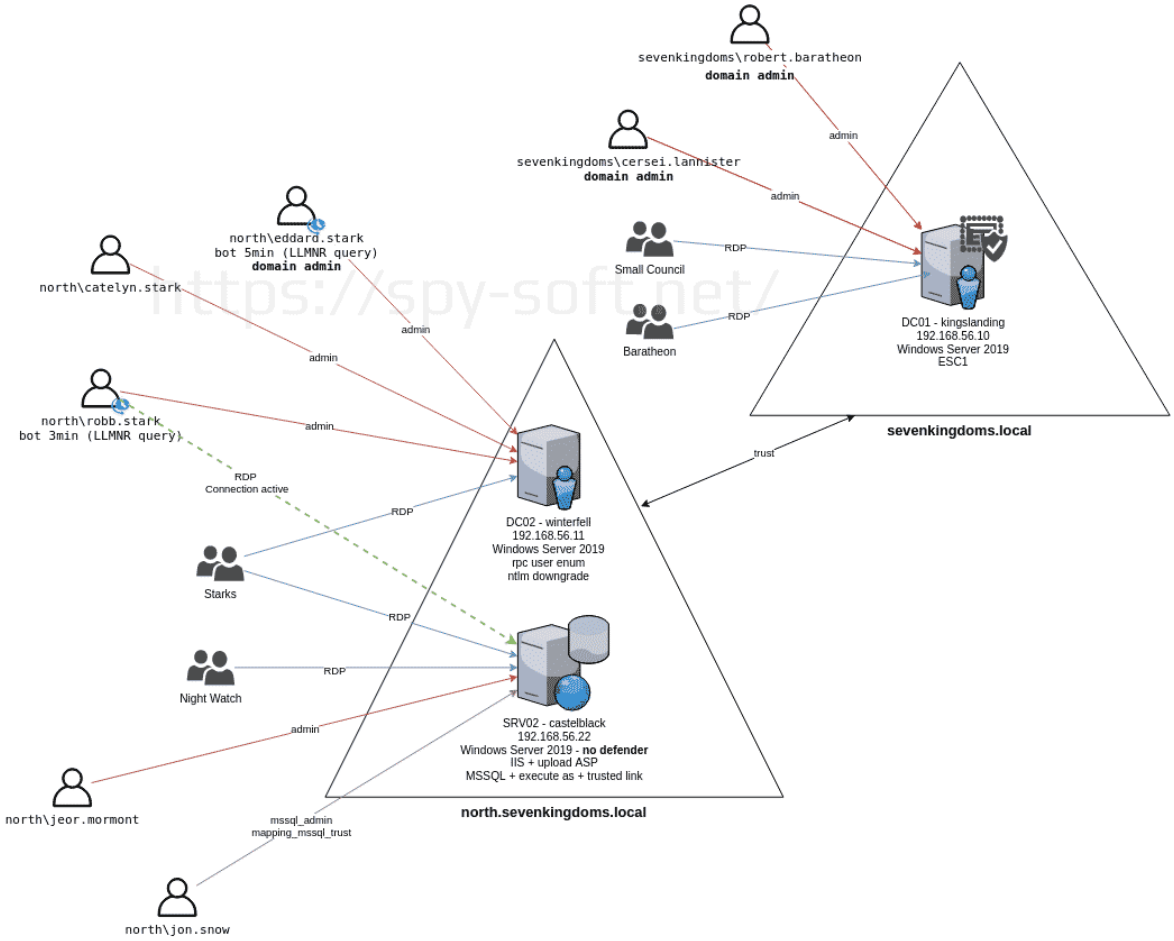
Доступны несколько вариантов лабораторий:

- **GOAD** — 5 виртуальных машин, 2 леса, 3 домена (полная лаборатория GOAD).

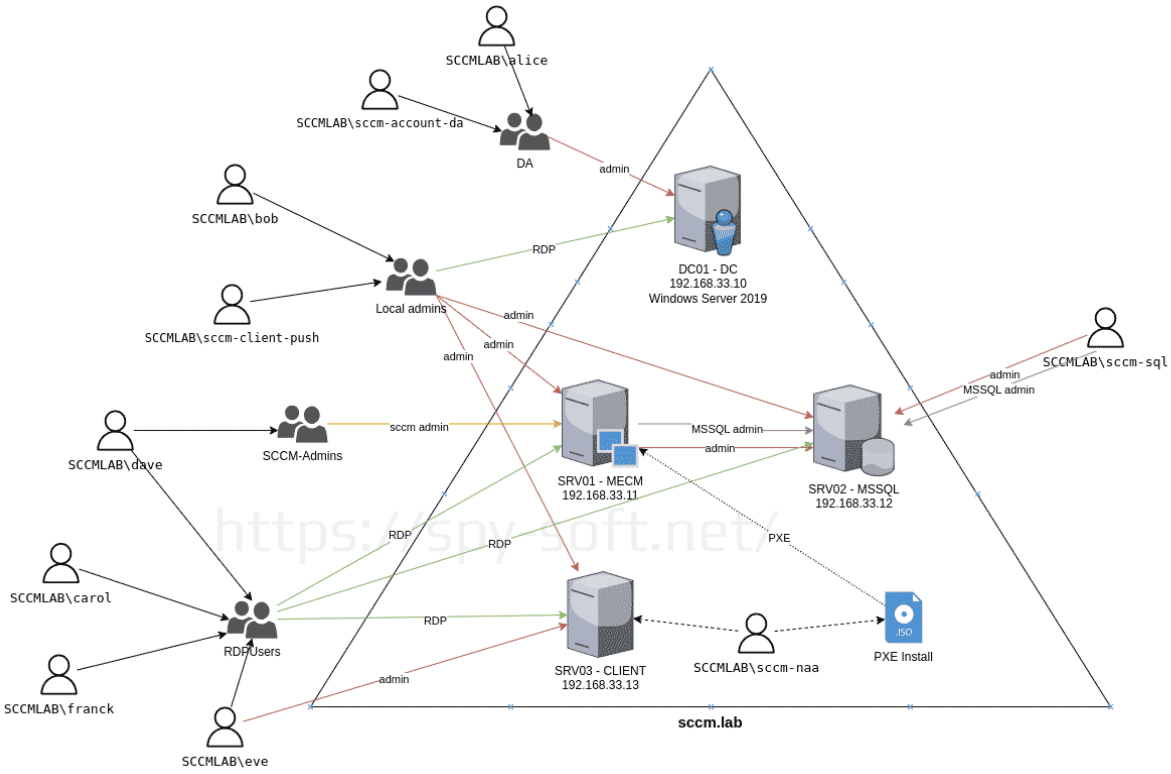
- **GOAD-Light** — 3 виртуальные машины, 1 лес, 2 домена (уменьшенная версия для менее мощных компьютеров).
- **MINILAB** — 2 виртуальные машины, 1 лес, 1 домен (базовая лаборатория с одним контроллером домена Windows Server 2019 и одной рабочей станцией Windows 10).
- **SCCM** — 4 виртуальные машины, 1 лес, 1 домен, с установленным Microsoft Configuration Manager.
- **NHA** — испытание с 5 виртуальными машинами и 2 доменами, без предоставленной схемы — вам придется самостоятельно разобраться, как ее взломать.



GOAD — 5 виртуальных машин, 2 леса, 3 домена.



GOAD-Light — 3 виртуальные машины, 1 лес, 2 домена



SCCM — 4 виртуальные машины, 1 лес, 1 домен, с Microsoft Configuration Manager

Для установки лаборатории потребуется около 115 ГБ свободного места. Сама лаборатория занимает примерно 77 ГБ, но вам также понадобится место для образов виртуальных машин Vagrant: Windows Server 2016 (22 ГБ), Windows Server 2019 (14 ГБ) и Ubuntu 18.04 (502 МБ).

Лаборатория предназначена для установки на Linux и тестировалась только в этой среде. Некоторым удалось установить ее на Windows, создав виртуальные машины с помощью Vagrant и выполнив часть подготовки Ansible с Linux-машины.

Для быстрой установки на Linux с уже установленными VirtualBox, Vagrant и Docker, выполните следующие команды:

```
./goad.sh -t check -l GOAD -p virtualbox -m docker
./goad.sh -t install -l GOAD -p virtualbox  -m docker
```

Теперь можно взять кофе — процесс займет некоторое время.

Для выборочной установки, следуйте соответствующему руководству для Virtualbox, VmWare, Proxmox или Azure.

GOAD — это отличный инструмент для всех, кто хочет улучшить свои навыки в области безопасности и пентеста Active Directory. Удачи в изучении техник атак!

ПОЛЕЗНЫЕ ССЫЛКИ:

- Атака RBCD для захвата домена Active Directory
- Как повысить привилегии при пентесте Active Directory
- Взлом сети через групповые политики Active Directory