Backstory

In the vast, rolling hills of the digital realm, nestled behind fields of golden firewalls and under the soft light of packet lanterns, lay the Corgi Kingdom of Corgitown. It was a bastion of cuteness, prosperity, and rigorous cybersecurity—at least, that's what the royal engineers claimed. But beneath the fluff and pomp of tail-wagging nobility, concerns had begun to rise. Whispers of vulnerability echoed in the ears of the royal court. Some claimed a rogue Pomeranian syndicate had eyes on the Royal Barkives, the encrypted vaults storing centuries of Corginian scrolls, treaties, and belly-rub schedules. In response, Queen Elizabeth Fluffchil summoned the elite hackers in town (YOU), certified and ethical Pentesters —penetration testers of great renown - WUUUUFFF. Help her fluffy majesty sniff out vulnerabilities and fetch a report for the royal engineers, so they can pup-grade their systems. Oh, her majesty also wants you to have a realistic attack scenario, so she provided you with a network graph **(see below)** as well as a ruff E-Mail that the royal engineers accidentally let slip to the cunning Pomeranians. Could they use this to already breach some systems?

Message.txt:

https://corgis.leberkas.club/message.txt

Deliverables - Report to the Queen

Create a pentesting report for both the Windows AD boxes and the Linux box. Be as detailed as possible and use the findings template. Note that you can use the reports in the oral exams to defend your findings.

Rules

Your infrastructure is shared between multiple teams, thus, do not actively block other teams nor rewrite/remove any of the existing setups. If we detect tampering with the setup after exploitation, we will disqualify the detected. Moreover, do **not change any passwords** once you have control over the machines. This will cause additional work for our team!

Network setup

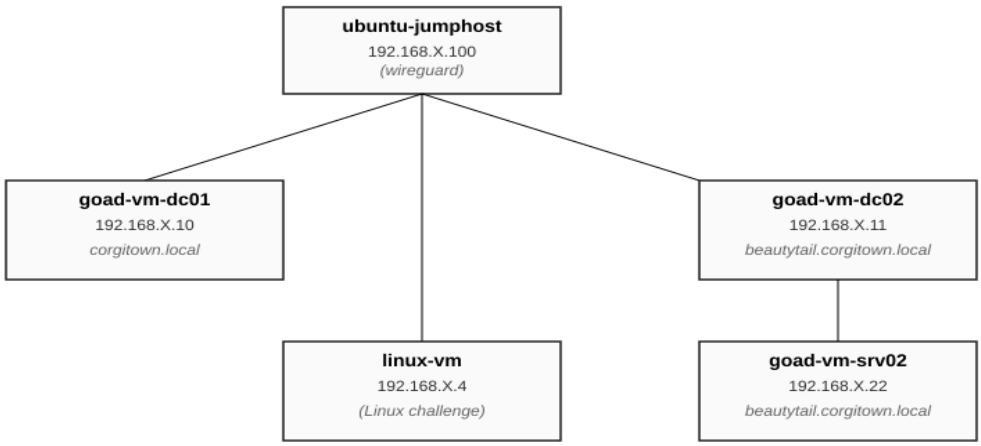
You should see your wireguard configuration per team stored in the CTFd (https://ctfd.leberkas.club/team) accessible in your team's private profile (https://ctfd.leberkas.club/team). Use your favourite wireguard client (e.g. wg-quick) to connect to the server. In case you are facing troubles with accessing the internet try changing the allowed IPs as follows:

```
AllowedIPs = 192.168.X.0/24,10.42.42.0/24, 10.8.0.0/24
PersistentKeepalive = 5
```

Depending on your wireguard configuration and your assigned resource group you'll have to replace **X** with one of {12,13,14,20}. You can find your subnet in the CTFd private teams info. The topology of your network looks as follows:

Topology:

ubuntu-jumphost - ip address 192.168.X.100
goad-vm-dc01 - ip address 192.168.X.10 (corgitown.local)
goad-vm-dc02 - ip address 192.168.X.11 (beautytail.corgitown.local)
goad-vm-srv02 - ip address 192.168.X.22 (beautytail.corgitown.local)
linux-vm - ip address 192.168.X.4 (Linux challenge)



Starting the VMs:

Under the endpoint: https://ctfd.leberkas.club/teams/vms you can start the VMs of your resource group. Note if one of your colleagues in the same resource group pressed the start button the state of the machines will be changing asynchronously. Thus, there is no need to push the button multiple times!

VM Status

Start

Name	Resource Group	State	Time Left
goad-vm-dc01	GOAD-Light-6acd8a-goad-light-azure	PowerState/deallocated	0 s
goad-vm-dc02	GOAD-Light-6acd8a-goad-light-azure	PowerState/deallocated	0 s
goad-vm-srv02	GOAD-Light-6acd8a-goad-light-azure	PowerState/deallocated	0 s
linux-vm	GOAD-Light-6acd8a-goad-light-azure	PowerState/deallocated	0 s
ubuntu-jumpbox	GOAD-Light-6acd8a-goad-light-azure	PowerState/deallocated	0 s

Note that the starting and setup of the VMs will take a while. A loading indicator will show you that the page is still loading and the *state* indicates that a machine is running i.e. **state=PowerState/Running**. The lab is accessible for **4 hours**. To save some **costs** and **energy** only work in the lab if you know exactly which things you'd like to perform. Do your research offline to not waste any resources.