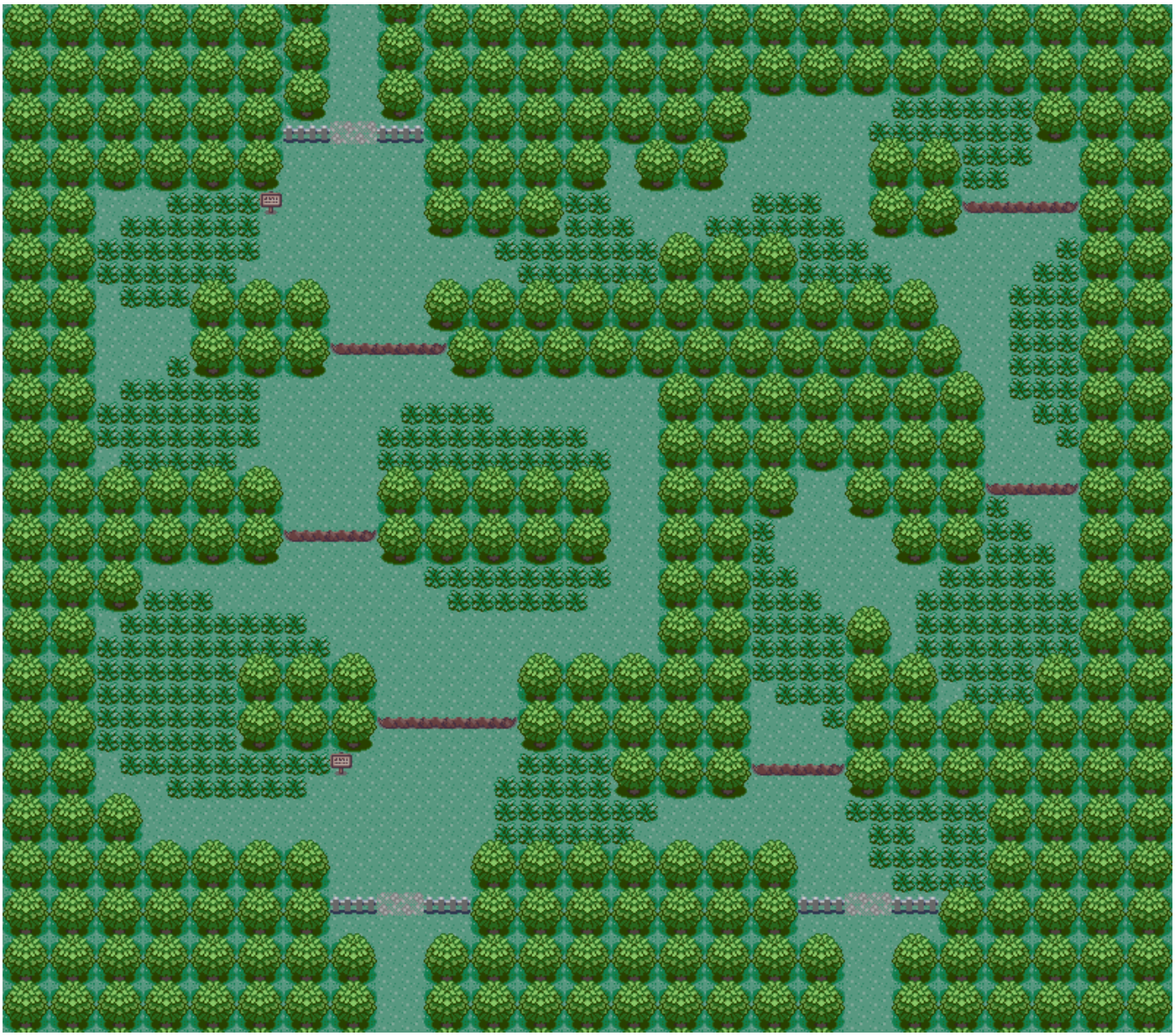
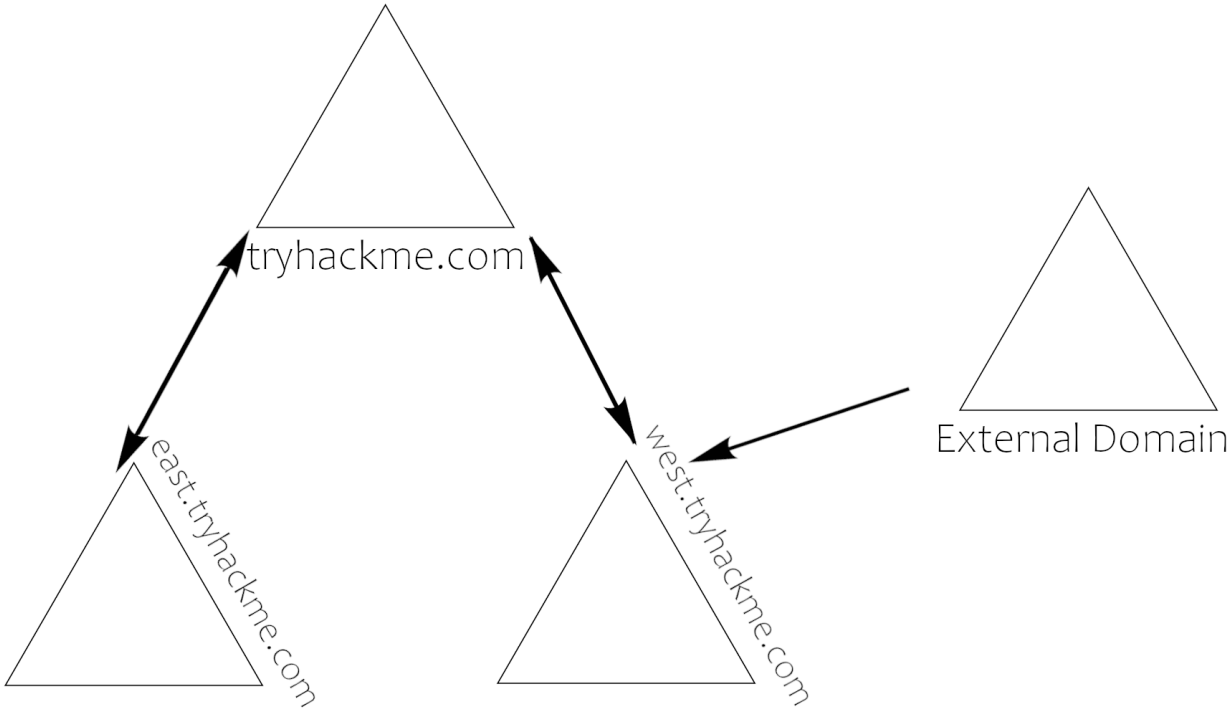
# 31

Now that we have dumped credentials on the primary domain controller we can utilize these credentials to find other domains or forests that we can gain a foothold on. We can begin by using offensive powershell or bloodhound to find a forest trust then use credentials to access a segmented domain controller.



Domain Trusts Overview

Trusts are a mechanism in place for users in the network to gain access to other resources in the domain. For the most part, trusts outline the way that the domains inside of a forest communicate to each other, in some environments trusts can be extended out to external domains and even forests in some cases.




*Trusts forest visual*

There are two types of trusts that determine how the domain communicate. Find an outline of the trusts below.
• Directional - The direction of the trusts flows from a trusting domain to a trusted domain.
• Transitive - The trust relationship expands beyond just two domains to include other trusted domains.

The type of trusts put in place determines how the domains and trees in a forest are able to communicate and send data to and from each other when attacking an Active Directory environment you can sometimes abuse these trusts in order to move laterally throughout the network.

Hunting for an Attack Surface
We can utilize either offensive powershell or bloodhound, both give the same amount of information however they give different ways of presenting the data. Utilize powerview or bloodhound to enumerate the trusts within the network.

Crossing the Trust
We can utilize a trust just like there was a user on the domain controller itself. The second domain will authenticate with the primary domain controller to allow access to the server.
Make sure that you have a proxy server running on THROWBACK-DC01 to use proxychains and pivot to the corporate environment.
Options to pivot across the trust

```
proxychains ssh MercerH@10.200.x.118
proxychains xfreerdp /u:MercerH /p:'' /v:10.200.x.118
```

Answer the questions below

What domain has a trust relationship with THROWBACK.local?

Submit

What is the hostname of the machine that has a forest trust with the domain controller?

Submit

What is the Administrator account we can use to access the second forest?

Submit

What is the name of the file in the Administrator's Documents folder?

Submit

Submit flags for CORP-DC01 in Task 4

Completed