BloodHound

enumeration tool that shows attacks and relations in an active directory environment . (attack map)

- upload sharphound to target windows machine , exe or ps1 (power shell script)
- run it --> generate bloodhound.zip file --> download it on ur kali
- drag and drop this zip file to bloodhoind

-To run the ps1

```
import-module .\SharpHound.ps1
invoke-BloodHound -CollectionMethod All
```

-To run the exe

```
.\SharpHound.exe -c all  -d active.htb --domaincontroller 10.10.10.100
```

bloodhound python tool : --> still need to know how to get its output (useless at the moment)

```
bloodhound-python -c All -u <username> -p <password>  -d egotistical-bank.local  -ns 10.10.10.175
```