# HACKTHEBOX

# ACTIVE DIRECTORY BLOODHOUND
# CHEAT SHEET

| Command | Description |
|---|---|
| `xfreerdp /v:<target IP address> /u:htb-student /p:<password>` | RDP to lab target |
| `.\SharpHound.exe -c all --zipfilename inlanefreight_bloodhound` | Run the SharpHound C# ingestor |
| `Invoke-BloodHound -CollectionMethod all -ZipFileName ilfreight_bloodhound` | Run the SharpHound PowerShell ingestor |
| `bloodhound-python -dc <DC> -gc <GC> -d <DOMAIN> -c All -u <user>` | Run bloodhound-python |
| `xfreerdp /v:10.129.2.43 /u:htb-student /drive:data,/tmp` | Transfer data to and from the target host with drive redirection |