حمله به Active Directory راهی عالی برای دستیابی به کنترل یک محیط است ، به شما امکان می دهد به داده ها دسترسی پیدا کنید و بر اساس اهداف خود عمل کنید. BloodHound به شما امکان می دهد کوتاهترین مسیر را برای رسیدن به مکان مورد نیاز خود تجسم کنید. درک رابطه بین هزاران Active Directory ممکن است دشوار باشد. کاربران اعضای گروه هایی هستند که می توانند در گروه های دیگر قرار بگیرند و به هزاران مجوز پیوند داده شوند. در این دوره ، Discovery with BloodHound ، شما توانایی استفاده از BloodHound را خواهید یافت تا سریعاً کوتاهترین مسیر برای به خطر انداختن سیستم ها را در یک محیط Active Directory پیدا کنید.

ابزارBloodHound:

BloodHound از نظریه گراف برای آشکار کردن روابط پنهان و اغلب ناخواسته در یک محیط Active Directory استفاده می نماید. مهاجمان می توانند از BloodHound برای شناسایی آسان مسیرهای حمله بسیار پیچیده استفاده کنند که در غیر این صورت شناسایی سریع آنها غیرممکن است.   
مدافعان می توانند از BloodHound برای شناسایی و حذف همان مسیرهای حمله استفاده کنند.

هر دو تیم آبی و قرمز می توانند از BloodHound استفاده کنند تا به راحتی درک عمیق تری از روابط امتیازات در یک محیط Active Directory به دست آورند.

برای اینکه ابزار را تست نمایید پیشنهاد می شود آن را در ماشین کالی خود نصب نمایید. برای نصب آن مراحل زیر را انجام دهید:

1) sudo apt install bloodhound -y

2) sudo pip3 install bloodhound ( if you don't have pip3, you shoud install pip3 first)

3) sudo neo4j console  (To create database)

or

4) install training database from this [link](https://github.com/BloodHoundAD/BloodHound-Tools/tree/master/DBCreator).

5) sudo bloodhound-python -u -p -ns -d

6) Finally you have json output