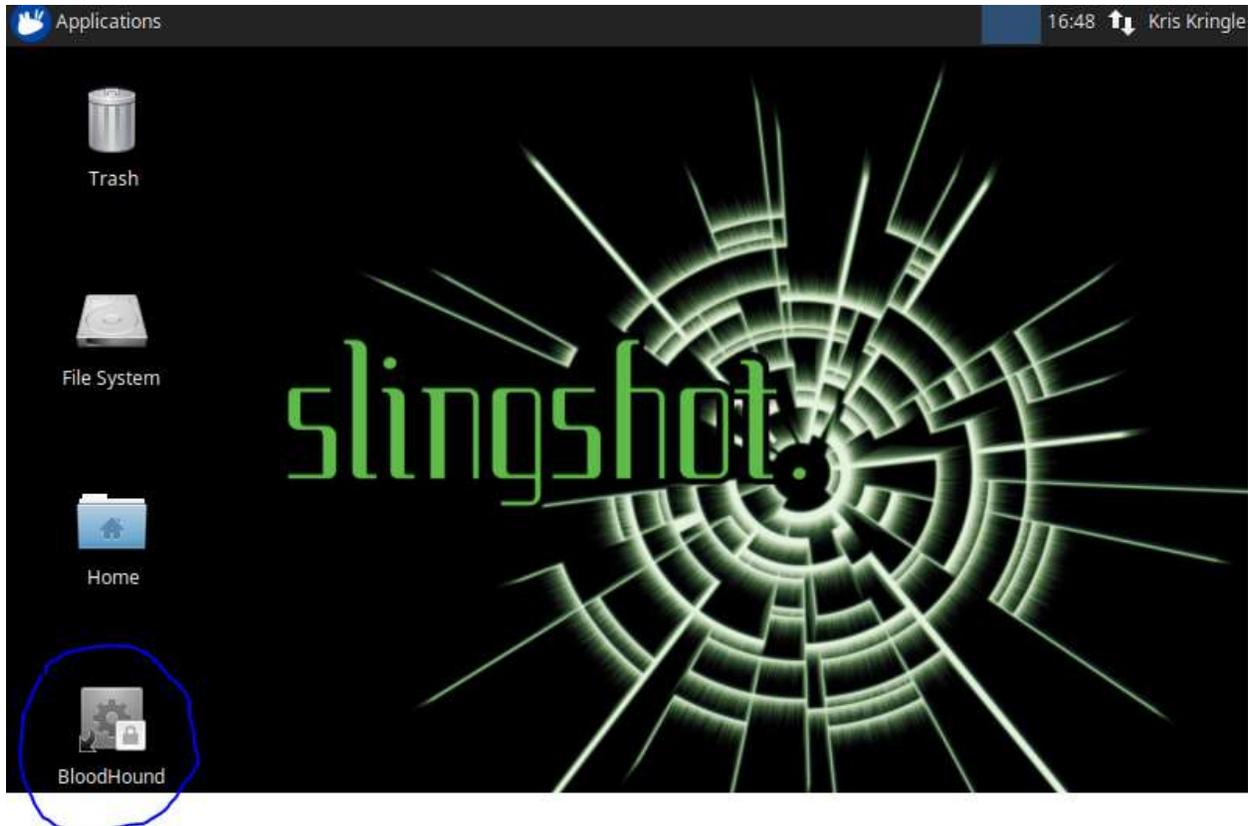


Objective--AD Privilege Discovery (Part 2)

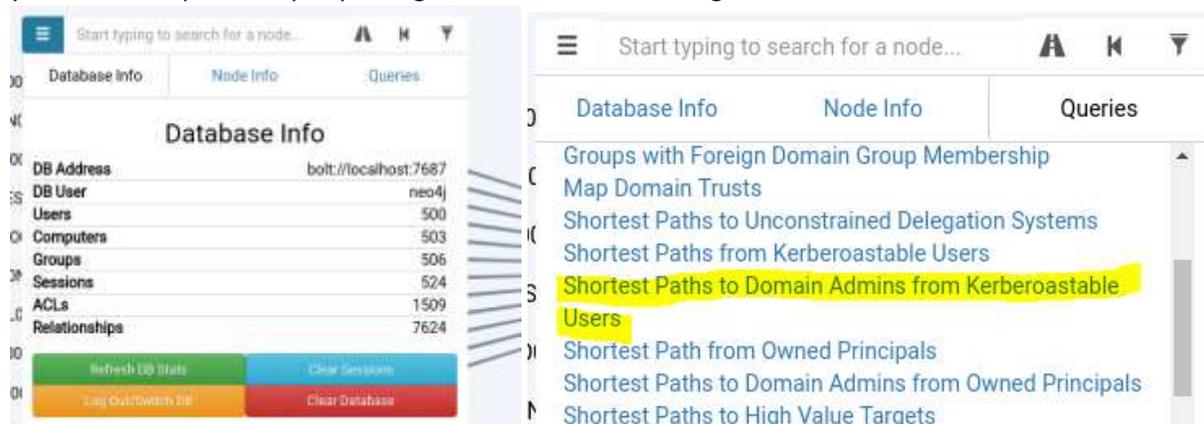
Solution

The hardest part to this challenge is getting the virtual machine to run. Although the SANS/CounterHack designers designed the VM to run on as many hypervisors as possible, some players had problems. Here, we are running the VM on VMware Workstation v15.

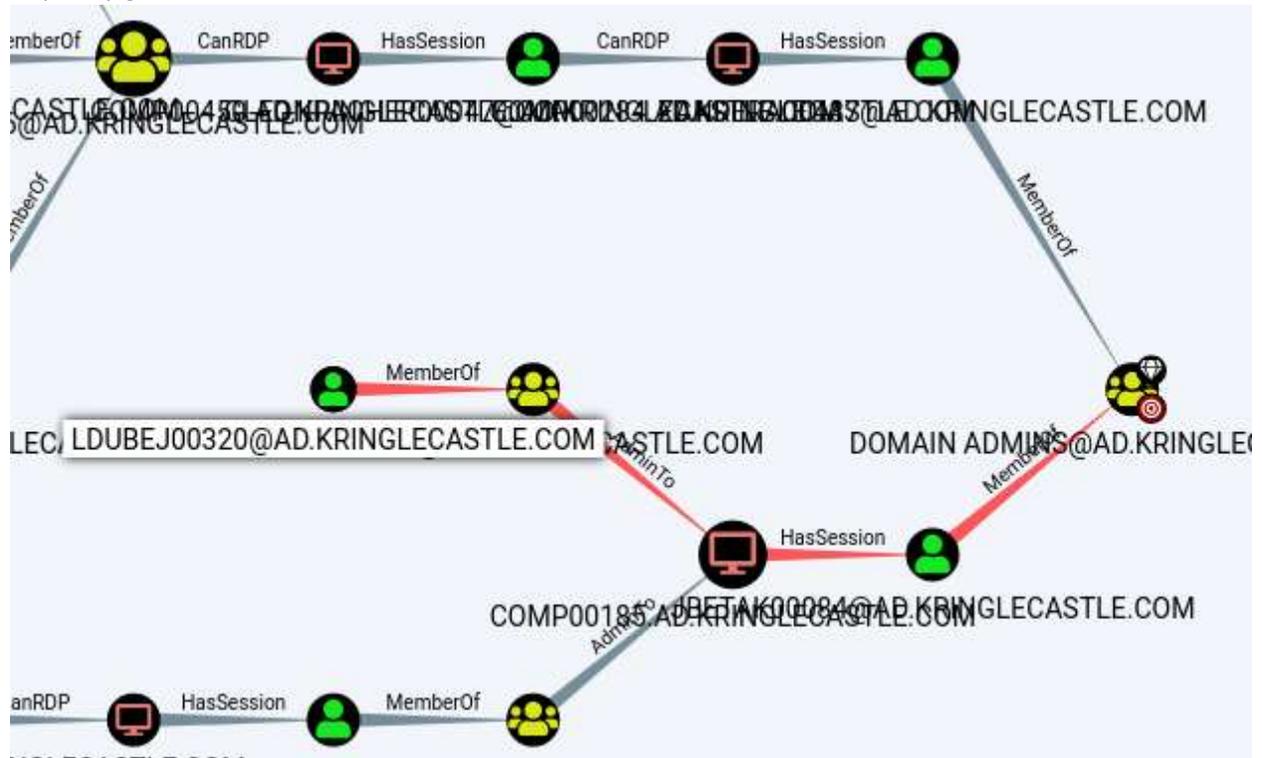
Once the VM is running, open the BloodHound application.



As in the demonstration, click on the menu/sandwich icon at the top left. When you click on Queries you will find a prebuilt query that gives us what the challenge asked for.



It quickly give us the answer we seek.



```
5) AD Privilege Discovery
Difficulty: 🚩🚩🚩🌲

Using the data set contained in this SANS Slingshot
Linux image, find a reliable path from a
Kerberoastable user to the Domain Admins group.
What's the user's logon name? Remember to avoid RDP
as a control path as it depends on separate local
privilege escalation flaws. For hints on achieving
this objective, please visit Holly Evergreen and help
her with the CURLing Master Cranberry Pi terminal
challenge.

LDUBEJ00320@AD.KRINGLECASTLE.COM Submit
```

Lesson Learned

A good penetration tester, or someone on IT staff who takes the time to learn to use these tools can help the organization [reduce its exposure to pass the hash attacks](#) and lateral movement.

Up Next

The next objective, Badge Manipulation, tells us we need to get hints by helping Pepper Mintstix solve the Yule Log Analysis terminal. Pepper is on the right wing of the second floor, beyond Tangle Coalbox and the Speaker Unpreparedness room. See you there!