

Objective--AD Privilege Discovery (Part 1)

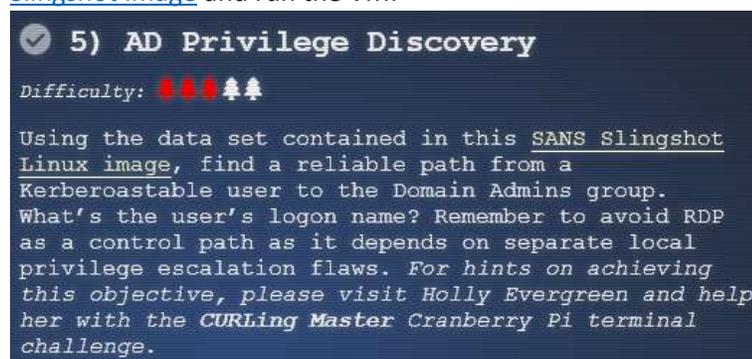
What you can learn from this

In its default configuration, a Windows Active Directory (AD) Domain is vulnerable to many attacks that can steal credentials, [NTLM hashes](#), or [Kerberos tickets](#). Some of the attacks [exploit obsolete protocols](#) like NETBIOS, others [extract hashes from memory](#) and use them in attacks called [pass the hash](#) or [pass the ticket](#). Once attackers compromise one host in a Windows domain, their goal is compromise other hosts in the domain in search of sensitive information or domain administrator credentials. This is known as lateral movement.

This objective highlights a tool that helps the penetration tester navigate the path from a compromised host in a Windows domain to a host with domain administrator access.

Getting Started

The objective gives a link to a Linux image that has the Bloodhound application installed. The image works in [VMware Workstation Player](#) v15, in current versions of [VMware Fusion](#) for Mac, and in [VBox](#) (in VBox, you must change the OS selection from Debian 32 to Debian 64 for it to load.) Download the [Slingshot image](#) and run the VM.



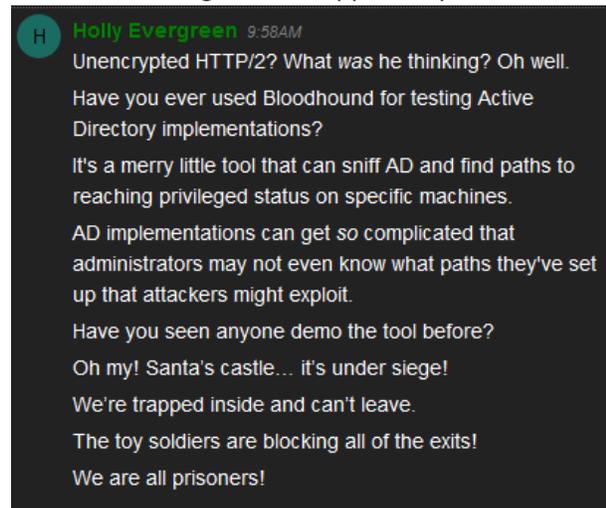
Hints

After you solve Holly Evergreen's terminal and talk to her, there will be two new hints in your badge. The first is a link to [Bloodhound's GitHub repository](#), and the second is a link to [a YouTube presentation](#) on using Bloodhound. If you watch the YouTube presentation it will show you exactly how to solve this challenge.

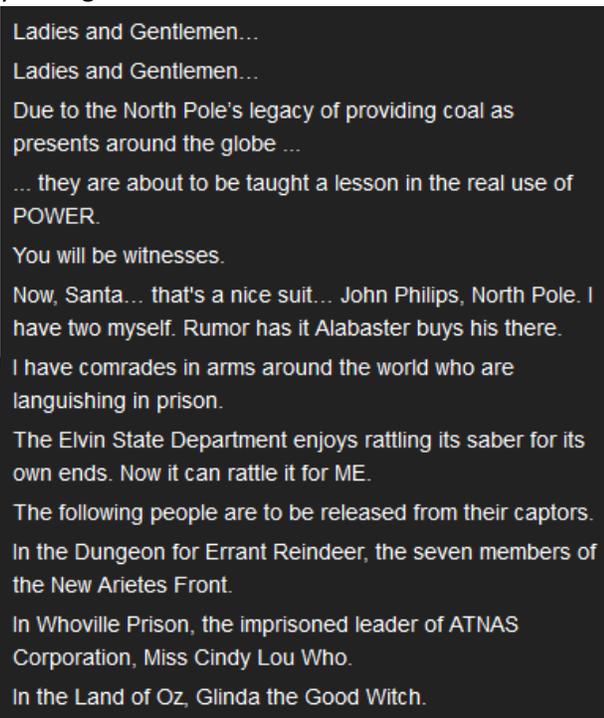


A Detour into the narrative

The elves are frightened. Apparently, the castle is under siege and we are all trapped in the castle.



If we talk to Hans (first floor lobby), a chilling story emerges.



We thought we were attending a conference at the North Pole, but we may have to save Santa and Christmas yet again!

Hand In

Install the virtual machine and follow the instructions in the YouTube demonstration of Bloodhound. Remember the caution about avoiding paths that involve RDP.

- 1) What is the login name of a user vulnerable to [Kerberoast](#) that will lead us to domain admin?