Ex0a0

Joshua Main-Smith

2020-10-21

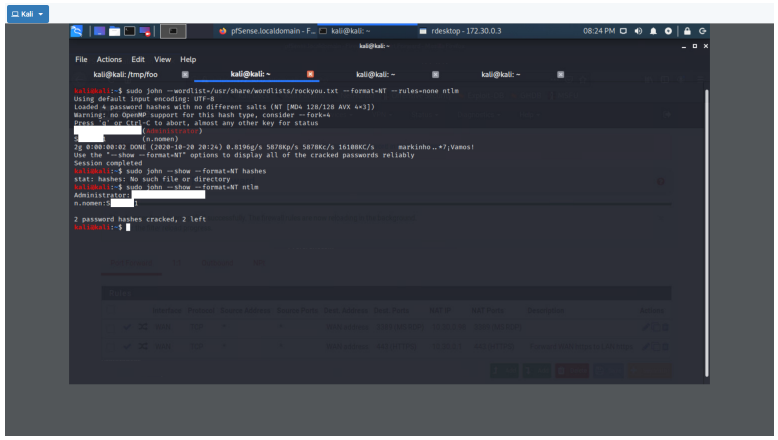
Contents

Attack Narrative

Hash Cracking with John The Ripper

With the hashes we got from Mimikatz on the Herd machine, we saved the hashes to our local machine to attempt to crack them using John the Ripper. We saved the hashes to a new file called **ntlm** with the format **user:hash** for each user on a new line.

We discovered two passwords using a dictionary attack against the hashes. A redacted screenshot of our findings can be seen below.



These findings can be found by using the commands **sudo john –wordlist =/usr/share/wordlists/rockyou.txt –format=NT –rules=none filename**. The passwords cracked can be seen using **sudo john –show –format=NT filename**.

Based on our reconnaissance from exploring Herd, one of these profiles appear to be from an inactive account. The other one may be inactive or is not part of a user group that allows Remote Desktop. The messages from these sign in attempts are shown in the images below.

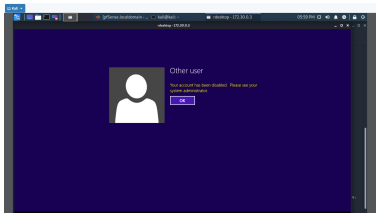


Figure 1: Admin Signin Attempt

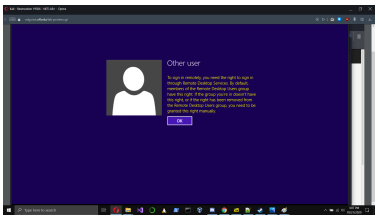


Figure 2: Nomen Signin Attempt

Zoom Links

October 21, 2020