Ex0a0 - HashTag

Simon Tobon

2021-07-08

Contents

Technical Report

Introduction

This Exercise was a very short Exercise, for this one we were tasked to crack as many hashes that we captured in the previous Exercise with John the Ripper.

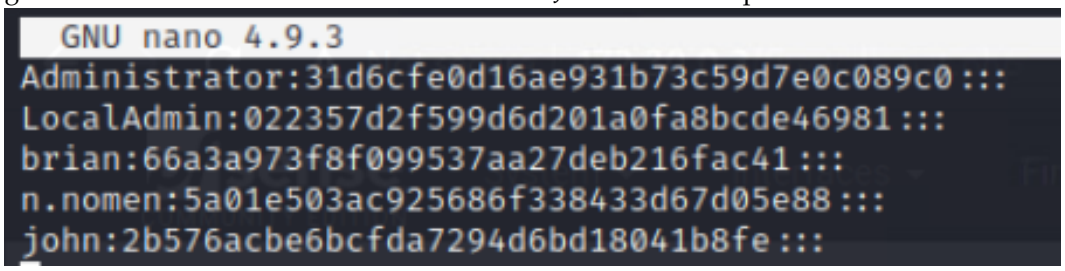
Finding: Description of finding

Vulnerability Description

These hashes can be cracked fairly easily making many Windows login profiles easy to enter.

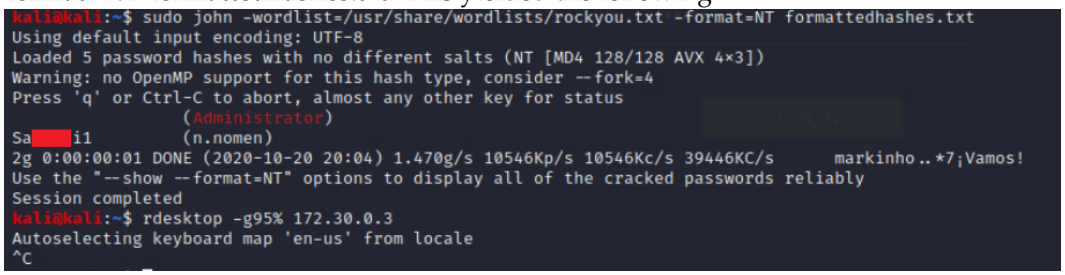
Attack Narrative

To begin I sftp'd into Plunder and retrieved the hashes.txt file from the previous exercise. **sftp stobon@plunder.pr0b3.com** I then copied the file over with get hashes.txt I then reformatted the hashes so John could interpret them:



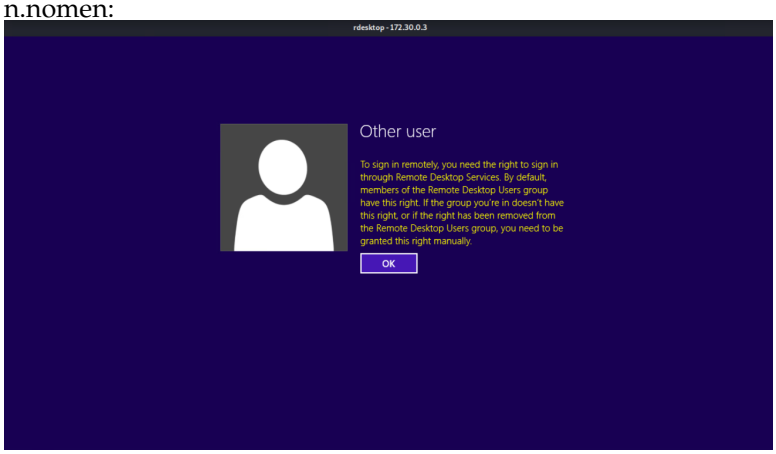
The syntax is user::hash.

Following this I ran **sudo john -wordlist=/usr/share/wordlists/rockyou.txt -format=NT formattedhashes.txt**. This yielded the following:

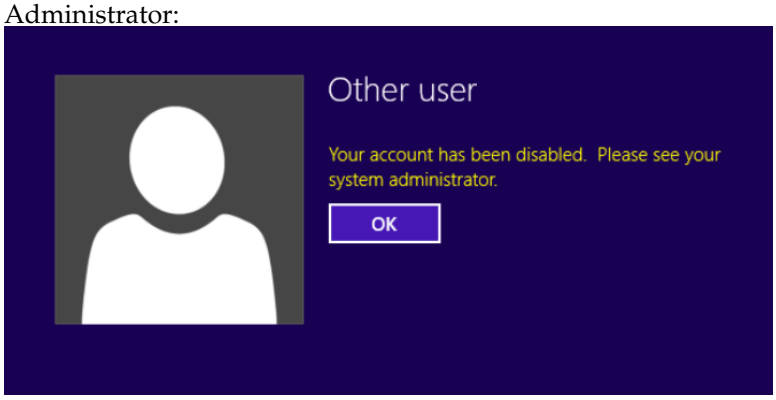


Note that parts of the password have been obscured for confidentiality, but you can conclude that it indeed was cracked. With these results we cracked both Administrator and n.nomen passwords. Administrator is no password, and n.nomen is Saxxxxi1. We can see that we are able to login:

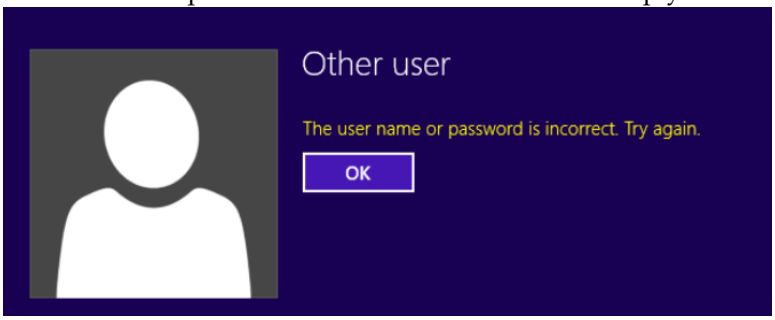
- n.nomen:



- Administrator:



Note that if the passwords were incorrect it would simply state:



There were no keys for this assignment, so we can conclude the report.