Contents

1 Introduction **1**

2 Active Directory Freebies **1**

3 Red Team Gimmicks **1**
3.1 Visitors 2
3.2 The Intern 2
3.3 Other devices in the room 2

1 Introduction

"I remembered how Albert Camus talks about the concept of resistance. The idea is that if you see that you cannot win, do everything in your power to resist. And that memory gave me the determination I needed." -Ding Liren

Assume everything is compromised. I think in the past, the red team has even had access to the laptops you are given. Be paranoid!

Assume the red team has fully gone through your public material and has the machines from your previous years. I know they have gloated in the past of busting teams when they reuse passwords across multiple years. They have a wordlist of all of the passwords used

One red teamer was gloating that he can enumarate all 12 character passwords in some short amount of time (6 hours?)

I am not sure if they make good use of it, but the red team does have the entire night to crack hashes. So make long passwords! This is probably especially relevant for windows, as kerberos uses hashes extensively. ¡update with more details¿

2 Active Directory Freebies

Disable all of the accounts besides the black teams and your own.

Change your password to something random and good.

At some point, you can make a new administrator account with an unusual username. You can keep the old account around as a honeypot if you want.

3 Red Team Gimmicks

"I was surprised by it, but I wasn't surprised that I was surprised. I expected a surprise, I just wasn't sure which one." -Fabiano Caruana

The red team loves gimmicks. It adds some fun and lets them be creative. So expect to be surprised.

3.1 Visitors

Visitors are malicious. If people walk in the room, cover your password sheets. I kept mine in my pocket and only took it out when I needed it.

3.2 The Intern

There is an intern, and they will be polite and unassuming. But their goal is to mess with you! Never take your eyes off the intern! They can try to plug USBs into your computers, take pictures with your password sheets (don't allow them to take any pictures). Apparently the intern and her handler will follow any rules you tell them. So tell them to not take picures, install unwanted programs, plug in devices, etc.

3.3 Other devices in the room

One time the red team got passwords by having a hidden camera in the room and viewing the passwords on the whiteboard. Be careful of physical devices in the room. I think there was speculation that a doll had a camera in it, idk.