Planning

August 24, 2023

Contents

1 Introduction

This document is dedicated to how to learn the material, what in the documents needs improving, and how to prepare for the competition.

Ironically, this section needs to be fleshed out more. It will be as time goes on. I think the most valuable thing is to edit it after your experience with the competition. Then we can figure out what we did wrong and what we need to improve on.

2 Practice

> Theory and practice are the same
> in theory, but not in practice
>
> Ben Finegold

2.1 Take notes from the red team

If you want to win, you must
understand why you have been
losing

Internet person

3 Incident Response Templates

We lost a lot of points due to a failure to do incident response. You should make a report for literally everything you do. They give a brief tempalte to use, you should use that.

My year we submitted one giant incident response and it was terrible. Make a lot of smaller ones, and submit them quickly.

4 Injects

Dance like no one is watching;
email like it may one day be read
aloud in a deposition.

Olivia Nuzzi

They do not like it if you joke in your response, even if they joke in their inject.

5 First Contact

I am speed

Lightning McQueen

Speed is very important. I am not sure of how long you have before the red team attacks you, but it is not more than 10-15 minutes. By this time, you should have removed all low hanging fruit so they do not mess you up before you can even begin.

This is my tentative starting plan for the 2024 competition:

1. Run initial scripts (5 min completion?)
2. Look around with Process Explorer

5.1 Initial Scripts

Your scripts should automate the menial work for you. This includes:

1. Clearing the autoruns, clearing the task scheduler, correcting the registry (and writing the changes down)
2. Setting up logs / confirming logs are set up.
3. Downloading antivirus programs
4. Disabling AD accounts (not the black team!)
5. Disabling all local accounts
6. Changing your password (and obfuscating it to negate keyloggers)
7. Booting all RDP & SSH users off of the machine (important, disabling accounts is not enough)
8. Removing GPO policies
9. Configuring the local firewall
10. Run Antivirueses (Norton Power Eraser & Kaspersky)