Contents

1 Introduction

"Manufacturer's protocol dictates I cannot be captured. I must be destroyed." - IG-11

This document is some of my ideas which have been scrutinized/rejected by the team. Please add your own ideas of creative things to try.

Guidelines: you can't hack the red team, they are out of scope.

In addition, there are horror stories of people being clever with honeypots and being targeted by the red team. It is not really fair, but if you piss off the red team they will come for you and you will lose. Just take it into account.

2 Anti-Keylogger

The threat is stronger than the execution

Aaron Nimzowitsch

I remember in the team's practices, the mere idea that the passwords I was typing were being logged caused me distress. Did the attacker know the password I had just changed? Their keylogger did not work, but it got me thinking of how to combat them.

There are many types of loggers, which can log your clipboard, and many other things. Somehow they get into your drivers, don't ask me. (But I would like to learn)

Our goal is to be able to type securely into a compromised machine. To this end, I have made a program which types random characters. There are many possibilities for this

3 Honeypots

You can make honeypots, but it is not advised.

3.1 Honeypot Kerberoasting

4 Reverse Shells

There are many reasons why this is a bad idea. You are installing malware on your computer. You are allowing the traffic through your firewall.

However, a reverse shell would allow you to maintain persistent access to the machine if the attacker locks you out. As we are only competing for a few hours, such access could be invaluable.

5 Disabling SSH

The only people trying to ssh into the machines are attackers with scripts, I use RDP for everything. It would be funny to leave the port open, but have a script to block access from any machine that tries to use SSH. However, the red team may be able to spoof a connection from your IP and get it blocked. Maybe you can have a white list with your IP on it so you don't get blocked?

This whole thing is made a moot point by teleport. But there has to be some creative way to block attackers.

6 Faking Score Checks

Don't do it.

But for a security competion, the score checking is really not robust. The checks should come from the black team account or another program inside the computer. You could cheat by simply using wireshark to observe the score check requests and your machine's responses.