Contents

1 Introduction

“Manufacturer’s protocol dictates I cannot be captured. I must be destroyed.”
- IG-11

We may lose So 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

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

5 Faking Score Checks

Obviously this is immoral, against the rules, etc. But it is probably possible. The scoring engine is ScoreStack, which checks for a response over the network.

You could cheat by simply using wireshark to observe the score check requests and your machine's responses.