Fringe Ideas

August 24, 2023

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 and 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. So take it into account. The red team also doesn't have to play by the rules. They can just DDOS you and you're dead.

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? It got me thinking of how to combat keyloggers.

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 as the red team gets angry. I think smaller honeypots would make them less angry, as opposed to making your entire infrastructure a honeypot.

3.1 Honeypot Kerberoasting

3.2 Canary Tokens

The idea is to place a file like "Credentials.txt" on your desktop. You set it up so that when the attacker reads the file, it notifies you of a breach. Maybe it can automatically ban the person that read the file.

To do this:

1. Make the file
2. Go to the file's properties. Security, advanced, auditing.
3. Add a new audit entry to notify on both successful and failed access attempts
4. To see the event, open the event viewer and look for events with the event ID 4663 (an attempt was made to access an object)
5. You can set up a scheduled task that watches the event log for specific events (like the access of your honeypot file) and sends you a notification or takes some action when they're found.

It can make it more convincing if you put the file in a folder. Maybe even have multiple files together?

TODO: Run WinPeas and see what folders it picks up on. I want to make a file that their automated tools would pick up on.

4 Reverse Shells

There are many reasons why this is a bad idea. You are installing malware on your computer. You are allowing malicious 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.

We can use a reverse shell that communicates over https and allow that in the firewall.

Somehow it needs to be not detected by the antivirus. There are many ways to obfuscate it, I think a fun one would be to translate the program into morse code.

Metasploit Docs

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.