CCDC

UAlbany

Spring 2018

**"Everybody has a plan until they get punched in the face."**

The red team does give us one small mercy: settling time. We are walking into a network already compromised, filled to the brim with backdoors and “goodies” for them to use. As such, it wouldn’t be much fun, (or educational), if they just bricked our computers before we can log on.

We don’t know how much time they give us, but **15 minutes** is a good guess, as it is short, but enough time for us to get settled. Thus this is our time. For 15 minutes we can have free reign without the constant pressure of the red team, and we need to have a **plan**:

* **Asset Discovery**
* **Asset Lockdown**
* **Asset Vulnerability Scan**
* **Network Monitoring & Log Management (Passive Info Gathering)**
* **Service Lockdown**
* **Service Triage**