**Initial Offering:**

Basically do a bunch of versions of this: <https://attack.mitre.org/wiki/Main_Page>

In a way that looks just like Red Canary’s [Atomic Red Team](https://github.com/redcanaryco/atomic-red-team)

Adversary Simulation/Emulation

[Sword Makers:](https://docs.google.com/document/d/11USEGi9Z0n3p12BuFeUAG3HcUeB0i8pQw2fX85ooZyY/edit)

One small benign script that executes and logs results of malware execution:

**Tools:**

Cobalt Strike

Cactus Torch: <https://github.com/mdsecactivebreach/CACTUSTORCH>

Canvas

Metasploit

Pupy

<https://github.com/glinares/Hephaestus>

* Windows Execute
  + Signed Executables
  + Backdoor Factory
  + Fileless
    - Script Based
      * JavaScript, HTA, VBA, PowerShell, Python
      * HTA
    - Injection
      * <https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process>
    - Registry Manipulation?
* Windows Escalate
  + [Elevate Kit](https://github.com/rsmudge/ElevateKit/tree/master/modules)
  + Old Days
    - Ms14-058
  + Bypass UAC
    - Uac-token-duplication
    - Uac-dll
  + Getsystem
  + Device Guard Bypass
    - <https://github.com/mattifestation/DeviceGuardBypassMitigationRules>
  + Power Up
  + Windows Privesc Check
* Windows Egress
  + Create a ton of data in one place
  + Zip a ton of data
  + Http
  + Https
  + Dns
  + Icmp
  + hybrid
* Windows Lateral Movement
  + PSEXEC
  + WMI
  + PS Remote
  + COM
  + RDP
  + Go-Fetch
  + Death Star Empire
  + Mini-katz -> PTH
  + Kerberoast
  + Responder
  + Exploit Scans
    - Old microsoft
    - SBs