Questions for 11/22 Meeting with GMU Capstone team

* Are you worried about sniffing the PCIE bus?
* Device level memory dump capabilities?
* Is the packer going to be able to generate our loaders, or will that be a separate executable? (Add keys, IP address, port info, etc.)
* Do you want a killcode to remove loader from a system?
* Do you want the payload encrypted at rest on the packer system?
* If we are implementing a keystore, what security on the packer system? How secure should it be? We just want to recycle our config format (key\_1=hello) and encrypt it?

**Diagram of Packer/Loader**

Packer

* Bootstrapping
  + Look for heartbeat
  + Load config file
    - Receive heartbeat port
    - Payload dir
    - Keystore (encrypted)
      * Session keys
      * Master binary
      * Startup key
* First screen options (at prompt)
  + Available Systems (status)
    - IP
    - Heartbeat (byte, is it calling home?)
    - How much memory is available
  + Available Payloads
    - ls/dir, scrape output for valid payload
  + Add new payload
    - cp [given] to payload dir, run AES
  + Send payload
    - Flag/args: save to disk or run exec auto
  + Generate loader\*\*\*
  + Manage systems\*\*\*

Loader

* Customization (Config or in compiled binaries header)
  + Keys it needs to start (bootstrap)
  + Packer IP
  + Packer port
  + Heartbeat wait **(TIME WILL HAVE TO BE STANDARD ON BOTH DEVICES… otherwise packer will think its down)**
  + Session startup wait
* Session startup
  + Use config to init key exchange and receive session key.
  + Send single use information
    - OS
    - Anything else?\*\*\* (total mem or hard drive space)
  + Begin heartbeat
* Continue heartbeat, wait for [sent payload] or [manage system]\*\*\*
  + Extract and **run payload in memory**
    - Check arguments
  + Manage system
    - Nuke
    - Config changes (e.g. packer IP changes)
    - Handle updates?\*\*\*

Loader-Installer

* Add new service
* Register as service
* Copy loader binary to disk

\*\*\*Is this required or unnecessary?