



EXPLORING C2: PART 2

“SOMETHING WORKS’ISH”

Rick Matthews
CSC 842
Cycle 6
Blue Team



Status

- Continue work from Cycle 3
- Actually have something that is somewhat functional but buggy
- Proof of Concept
- Have learned a lot, but there is a ton more
- Still very basic but feel significant progress from Cycle 3
- May have to re-write significant portion of code

Environment

- Python
- Ubuntu
- IA Lab
 - *3 Ubuntu VMs*
 - *1 server*
 - *2 clients*
 - *All on same network*

Functionality

- Multithreaded server
- Client
- Basic functionality
 - *Get list of Clients*
 - So clients know about other clients
 - *Get Server code*
 - Groundwork – later add functionality in case a client has to become the server

Future Work

- Resolve multiple client issue
- Need to research how to better handle multiple threads
 - *Server initiate commands to all clients*
 - *Server initiate commands to select clients*
- Implement suggestion of clients testing to see if server is available
- Remove clients from client list text file that disconnect or are unresponsive
- Add other functionality
 - *File transfer*
 - *DDOS*
 - *Scan for candidate client servers*
- Redundancy
 - *Server goes down, a client can step up as the server*

REVIEW CODE

&

DEMO