EXPLORING C2

Rick Matthews

CSC 842

Cycle 3

Blue Team

Background

- Not a developer
- Don’t know a lot about Python
- Not in infosec, so couldn’t think of any tools that would be helpful

Goals

- Learn!
  - *Different aspects of malware*
  - *Python*
- Interesting
- Fun
- 1 project to expand / enhance over the semester

C2 (Command and Control)

- Explored in CSC 840 and CSC 841
- Wanted to explore in more detail
- Incorporate other malware ideas
  - *Botnet activity*
  - *Worms – self propagation*
  - *Denial of Service (DOS)*
  - *Others / Suggestions*
- Redundancy
  - *Server goes down, a client can step up as the server*

Environment

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

Spectacular Failure

- Really not that spectacular, but a failure
- Didn’t allow enough time to get the multithreaded client / server to work correctly
- So no demo

Nominal Code

- Functions (once client and server issues are resolved)

```
#Keep a file of all client connections
def addClient(clientIP):
    file = open("clients.txt","a+")
    file.write(clientIP+"%d\r\n")
    file.close()
```

Nominal Code (cont.)

```
#Print all clients
def listClients():
    file = open("clients.txt","r")
    cline = file.readlines()
    for x in cline:
        print (x)
        file.close()
```

Other functions

Will build out once client / server issues are resolved

```
# retrieve all clients from list and send to each client
# so all clients "know" about eachother
def sendClients():
```

```
# send a command to a client
def sendCommand(command, clientIP):
```

Other functions (cont.)

```
# request a file from a client
def requestFile(file, clientIP):



# send a file from the server to the client
def sendFile(file, clientIP):
```