THIS IS MY TALK

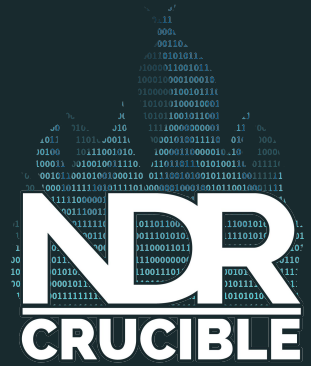
I'M WHITNEY

RECON INFOSEC

@shortxstack // unicorns.lol

OPEN SOC
NETWORK DEFENSE RANGE

- Lead Architect @ Recon InfoSec
- OpenSOC.io, Network Defense Range / Blue Team CTF
- DEF CON Blue Team Village
- #HackerTracker
- I make "art" (doo doo doo doo doo doo...)



BE HUNGRY TO LEARN

IT’S EASY TO TALK ABOUT WHAT YOU LOVE

IT STARTED WITH A SWITCH

ORIGINS OF OPENSOC

WORKING DOUBLE TIME

DEF CON 26

SO MANY VPNS

SO MANY FAILS

BIG GUNS

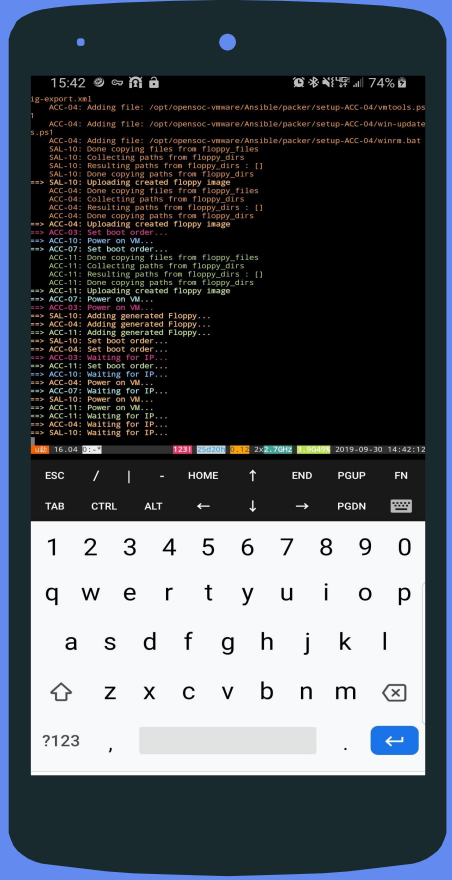
“That’s the sound of OpenSOC,
barreling through the casino…”

NDR CRUCIBLE

DEF CON 27

WAR STORIES

PHONE OPS



HYBRID ENVIRONMENT

$93,278

AMOUNT OF AWS $ SAVED

$9,259

AMOUNT OF $ SPENT ON FAILED HARD DRIVES

100%

SUCCESS

TAKEAWAYS

- Build a lab
- Learn all the things
- Break all the things
- Automate all the things (that need automating)
- HAVE FUN

STUFF TO CHECK OUT

- Packer
- Ansible
- Salt / SaltStack
- JuiceSSH
- DetectionLab
- ZeroTier
- Graylog
- Kolide
- osquery
- Moloch

blog.reconinfosec.com

blog.opensoc.io

THE END

QUESTIONS?

@shortxstack