Équipe Rouge:

The ethics of prosecuting an offensive security campaign

Hello!

I am Tarah Wheeler

I am here because I am a red team dork.

You can find me at @tarah and t@tarah.org

Hello!

I am Roy Iversen

I am here because I am also a red team dork.

You can find me at @royiversen

1

What's the point?

To charm, edutain, and argue with each other about the ethics of internal red teaming.

Why are we here?

INTRODUCTION

- Why do we red team? We are trying to keep people safe by pointing out flaws in security before parties unknown do
- What is this talk about and what will you know by the end of it.
- Where we go in the future.

WHY THIS TALK?

- We’re technical, not philosophers.
- Plenty laws on what’s legal and what’s not. Not enough open discussion on what’s OK vs not OK
- If we have no clear guidance, bad things can happen.

"A team is not a group of people who work together. A team is a group of people who trust each other."

-Simon Sinek

Red Team Retribution

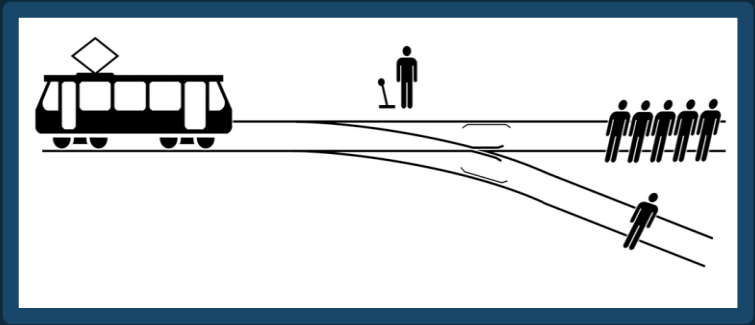
- Ever leave your laptop unlocked near your team?
- A tale of two victims

Where would *you* draw the line?

- Phishing user
- Insider threat
- Target the CEO
- Bribery
- Planting incriminating evidence

Crash course in Ethics

- Just because it’s legal, doesn’t make it OK (“ethical”)
- Ethics is complicated and context specific
- Right vs Right or Wrong vs Wrong



Conflicting responsibilities

- You might simultaneously have ethical responsibility to:
  - Demonstrate/prove risk to organization or client
  - Be excellent to your coworkers
  - Build trust in your team and profession

Theory vs Practice

- Tabletop Exercise

vs

- Seeing is believing

OK now what?

- The ethical boundary is context specific
  - We’re not here to give you the answer to what is right or wrong
- Let’s discuss where the line should be
  - Help people that are looking for guidance
  - Processes within your companies
- Internal teams vs External Teams

Please visit:

redteamsurvey.com

For the nascent *Red Team Ethical Framework* and poll results (soon), see:

https://redteamethics.com/ – *redirects to:* https://github.com/redteamethics

Thanks to...

Thanks to our friends, colleagues and family members who have guided us and put up with our many “what if” discussions.

Special thanks to:

Anna Fridley

Brian Genz

Deviant Ollam

Greg Conti

Paul Brandau

Zac Davis

Fortalice Solutions LLC and Splunk Inc

Sources and Resources

Research:

- Mouton, Francois & Malan, Mercia & Kimppa, Kai & Venter, H.s. (2015). Necessity for ethics in social engineering research. Computers & Security. 55. 114 - 127. 10.1016/j.cose.2015.09.001.
- Mouton, Francois & Malan, Mercia & Venter, H.s. (2013). Social Engineering from a Normative Ethics Perspective. 10.1109/ISSA.2013.6641064.
- Faily, Shamal & Iacob, Claudia & Field, Sarah. (2016). Ethical Hazards and Safeguards in Penetration Testing.
- "Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques"
- Mouton, Francois & Malan, Mercia & Leenen, Louise & Venter, H.s. (2014). Social Engineering Attack Framework. 10.1109/ISSA.2014.6950510.

Blog posts

- https://jacobian.org/writing/social-engineering-pentests/
- https://medium.com/starting-up-security/red-teams-6faa8d95f602

General social engineering resources of interest:

- https://opendatasecurity.io/the-most-famous-cases-of-social-engineering/

Any questions?

You can find us at:

- @royiversen
- @tarah

- shmoo@redteamethics.com

fin

END OF PRESENTATION