Tales from the trenches

An offensive security professional shares war stories, tips, and tricks from the red team

Dave Collins, Risk and Compliance Consultant

ACCUDATA® SYSTEMS
Secure. Modernize. Grow.

$whoami

- Husband
- Dad
- Academically trained historian
- GNU+Linux enthusiast (beard)
- Hacker (fuzzing, exploit development, CTFs/Boot2root/WarGames, writing code, professional tester of pens)
- Transplant from Washington state
- Professional background in network administration and web development
- Involved in InfoSec community (Greetz to Irvine Underground, @dc509, @spokane2600)
- Twitter: @whatever_sauce
- I'm from the internet so I <3 cat pictures!
- Shoutz to my employer as well as my coworker Andrew @boot2generic for reviewing this deck

Goals for the talk

- How to start a career in information security (brief)
- Share some bench hacking stories
- Provide some tips and tricks for securing home/biz
- Have some fun

Getting into InfoSec

Not the subject of the talk, but I wanted to share because I'm often asked:

- Help Desk -> Network Administration
- Entry-level SOC
- Junior Sysadmin / Data Center
- Developer or DevOps

Bench hacking stories

In the next section, I will share bench hacking stories from previous engagements

Bench hacking stories

Some caveats:

- First, none of these stories are from my time at Accudata – though my time with the firm has informed some of my suggestions.
- Second, names are excluded to protect all parties involved. In fact, any identifiable info has been removed.
- Finally, never pwn without permission! <hat color>

First story

Big fail followed by big win:

- First – big fail. Found vulnerability but blocked by firewall.
- Shoutz to the Shadowbrokers

First story: lessons learned

Lesson for red team: Always update your tools before leaving home

Lesson for blue: Block websites like exploitdb as well as Kali repo servers

Social engineering stories

Social engineering is one of the biggest threats to your organization. A few stories to scare/educate:

- Story: Evil LinkedIn account over 2,000 connections
- Story: Bad actors will attack anyone

Social engineering avoidance

- Tip: It’s cheap and easy to spoof a phone number – be skeptical!
- Tip: Ask for an extension to call back.
- Tip: Questions, questions, questions!

Cat break!

Everyone having fun?

Any questions yet?

Third story: “pentest” blues

Confusion about terms, small scope, no approval

Result: Bad news

If you decide to commit to a PT – actually get one

Tips to avoid trouble

- Tips for blue teams: Err on the side of “yes” for scope – bigger is better!
- Tips for red teams: Be insistent in scoping meetings

From Twitter – “A small scope is like saying you can only test one segment of body armor”

Tips and tricks

In this next section, I’m going to share some tips and tricks for your professional network, to avoid being socially engineered, and to improve your overall personal security.

Tips and tricks - Network

Here are some tips to help improve your network security:

- If your server operating system is more than 10 years old, the time to upgrade is now
- Try to turn off noisy/chatty protocols
- Ensure proper network segmentation

More network security tips

Here are a few more network security tips:

- Security awareness / business continuity / disaster recovery / asset inventory
- Least privileges model
- Ensure proper policies are in place (employee termination, multi-factor authentication, BYOD)

Tips and tricks - SE

Here are some tips to avoid being socially engineered:

- Always be skeptical
- Ask for their extension (phone)
- Don’t accept any/all LinkedIn requests
- If it sounds too good to be true – it probably is

Tips and tricks - personal

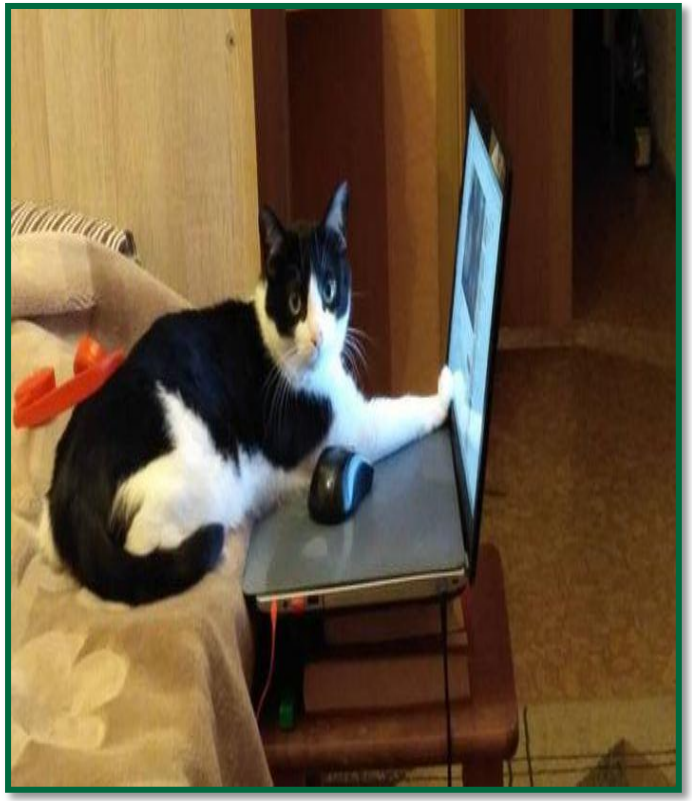
Here are some tips and tricks to help make sure your personal affairs remain secure:

- You don’t get phone calls from the IRS/Apple/Microsoft
- Install those Microsoft updates
- Be careful with pirated software

More personal tips

A few more personal tips:

- Exercise caution with public wireless
- Don’t trust “unhackable” products
- Generate hard passwords / password manager (| : ;)



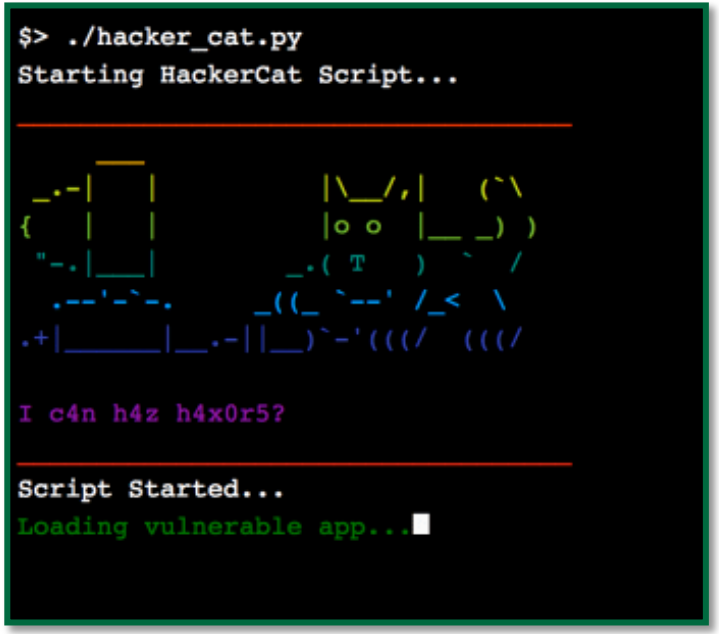
Attribution

Here's where I found all the cool cat pix:

- https://www.buzzfeed.com/expresident/best-cat-pictures
- https://www.youtube.com/watch?v=4dVV3GuIYBs – DJ Cat
- https://giphy.com/gifs/dancing-party-w5eFyOHmkS8uc - Giphy for the DJ Cat
- http://www.funnycatsite.com – Some of the final cat pictures came from this site
- https://imgur.com/gallery/7ok4g - Hacker cat came from this Imgur gallery
- https://inteact.act.edu.au/2017/04/10/art-of-cyber-security-exploitation-10am-1pm-on-29-april-by-women-in-tech/ - The last picture from the next slide came from here
- https://knowyourmeme.com/photos/1166375-hang-in-there-baby ---------->
- http://amazing-creature.blogspot.com/2018/01/funny-cats-part-293-40-pics-10-gifs.html#.XSYQgDBlDcs
- https://amazing-creature.blogspot.com/2017/12/funny-cats-part-288-40-pics-10-gifs.html#.XSYZSXdFzcu

Questions?

- If your server operating system is more than 10 years old, the time has come to upgrade
- Try to turn off noisy/chatty protocols
- Ensure proper network segmentation
- Security awareness / BCDR / essentials
- Least privileges model
- Ensure proper policies are in place (employee termination, MFA, BYOD)
- Always be skeptical
- Ask for their extension
- Don’t just accept any LinkedIn request
- If it sounds too good to be true – it probably is
- You don’t get phone calls from the IRS/Apple/Microsoft
- Be careful with pirated software
- Exercise caution with public wireless
- Don’t trust “unhackable” products
- Generate hard passwords / PWM




THANK YOU
FOR YOUR ATTENTION
quickmeme.com