This Will Never Work...

Derek Rook

2019 SANS SOC Summit
• Part time wizard
• OffSec Team Lead
• Bug Bounty...er? Bug Bounty Hunter?
• Recovering Systems Engineer
• Recovering Security Engineer
Disclaimer: Views are based on my own thoughts and experiences and do not reflect those of my employer
BONUS DISCLAIMER!!!!
Examples are based on real events, but have been abstracted to protect clients, hide origins, and keep you guessing!
Agenda

• Tell silly stories
• Get at least one laugh
• Maybe learn something
Explicitly Allow...INDEFINITELY!
derek.rook: So, we're actually kind of expecting this to fail, given flags `psexec` and we're using a default payload. If it does catch it, we'd like to reset and use an obfuscated payload.

derek.rook: nm, it worked out of the box
Explicitly Allowing Questionable Payloads

• PsExec isn’t inherently bad
• Unintentional consequences
• Any exception should be time bound
• Exceptions should be audited
Who's on First?
SO YOU WERE LOOKING FOR A GOLDEN CARP?

HE WENT THAT WAY OR THAT WAY
HE WENT THAT WAY

BUT IT'S NOT MY BUSINESS LOL
The only problem is, I can't remember what I've forgotten.
Not My Job-ism

- No one saw value/impact till too late
- Wasted lots of time/money
- Took lots of escalating to fix
- Clear communication of expectations
- RACI/PARIS/DACI/etc
Please Excuse My Dear Aunt Sally
PEMDAS IS MORE LIKE GUIDELINES THAN ACTUAL RULES
What’s The Point?

• Things to think about
• Partnership with OffSec
• As old Mad Eye would say...
CONSTANT VIGILANCE!
Thank You!
https://twitter.com/_r00k_
https://youtube.com/derekrook
https://gitlab.com/r00k