Being Offensive in the Workplace

Derek Rook
Views and opinions are my own and do not necessarily reflect those of my employer.
A Little About Me...

• 18+ year tech career
• OSCP, GWAPT, GCIA, etc
• 501st Legion Member
• Practice Kendo
Our Goal

• Maximize value from conferences
• Grow greater offensive capabilities
• Build stronger defensive posture
• Have more fun!
Getting Buy-in: Your Peers
Security Awareness: Offensive demo

• Be flashy
  • Turn on the webcam
  • Search for tax returns, passwords.doc, etc
  • Password cracking

• Don’t get too technical

• Show your passion!
Lock Pick Village

• Looking for that “Oh My!” moment
• Get people excited
• Get people used to engaging you
• Start recruiting
Getting Buy-in: Your Boss
You Best Come Correct

• Have a specific goal
  • 10% of your time? 20%?

• Bring measurable facts
  • Raised engagement after activities

• Have a plan
  • Start small, grow scope as value is demonstrated

• DEMONSTRATE VALUE!!!!
Time to execute!
Build Out Operational Maturity

• Identify gaps
• Highlight areas for improvement
• Illustrate potential impact
• Help remediate
• Establish security programs
Turn Phishing to 11

• Create payloads
• Phish alternate channels (slack, etc)
• Level up WITH the org
Physical Penetration Test

• Get those lock pickers
• Break into the office
• Look for unlocked computers
• Take notes
• Generate a real report
It Bears Repeating

• Start small and basic
• Grow as the org grows
• Show value at every step
• Have fun (it’s infectious!)
Thank You!

Derek Rook
https://r00k.io
https://twitter.com/_r00k_
https://youtube.com/derekrook
https://github.com/r00k5A58