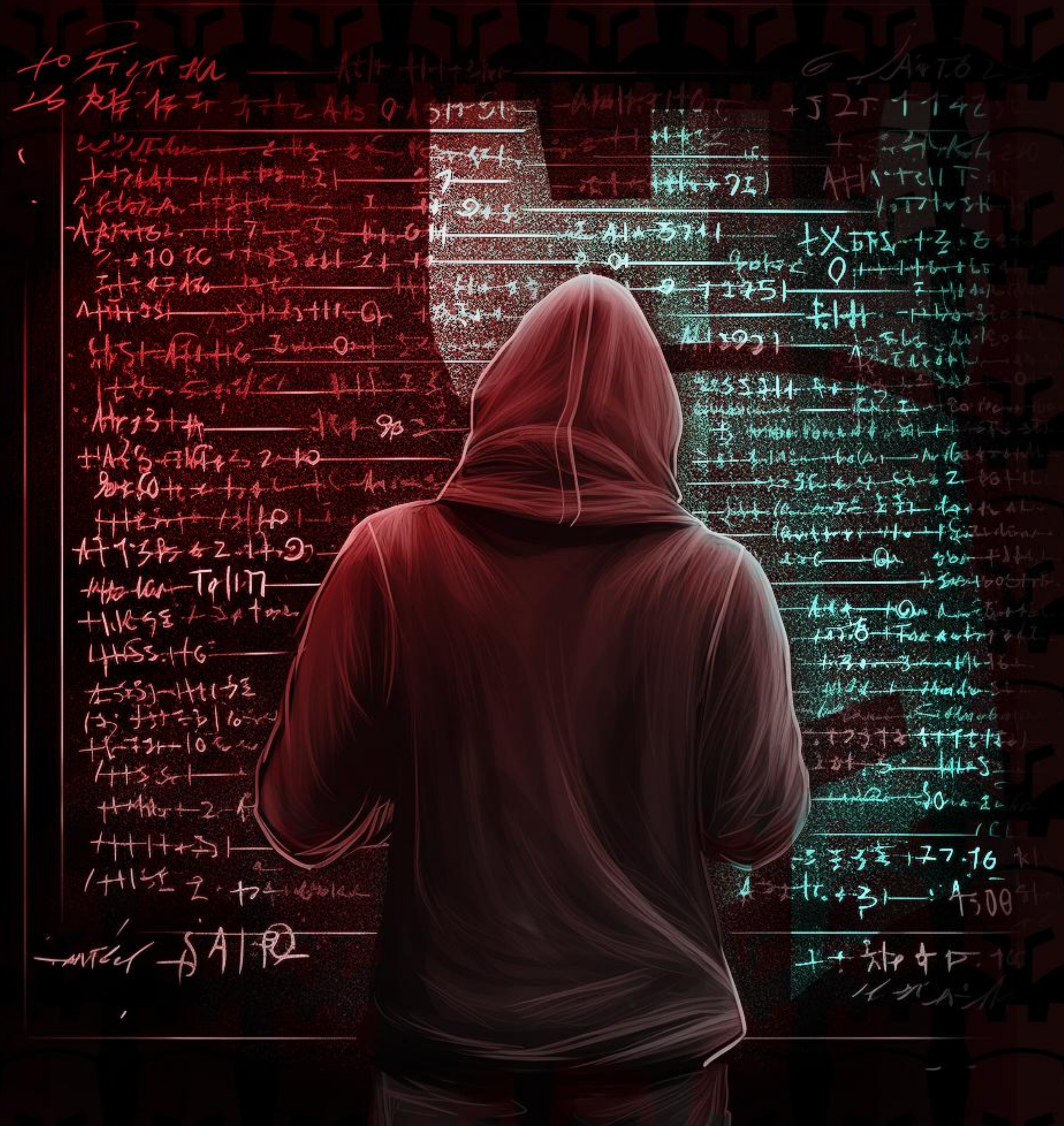


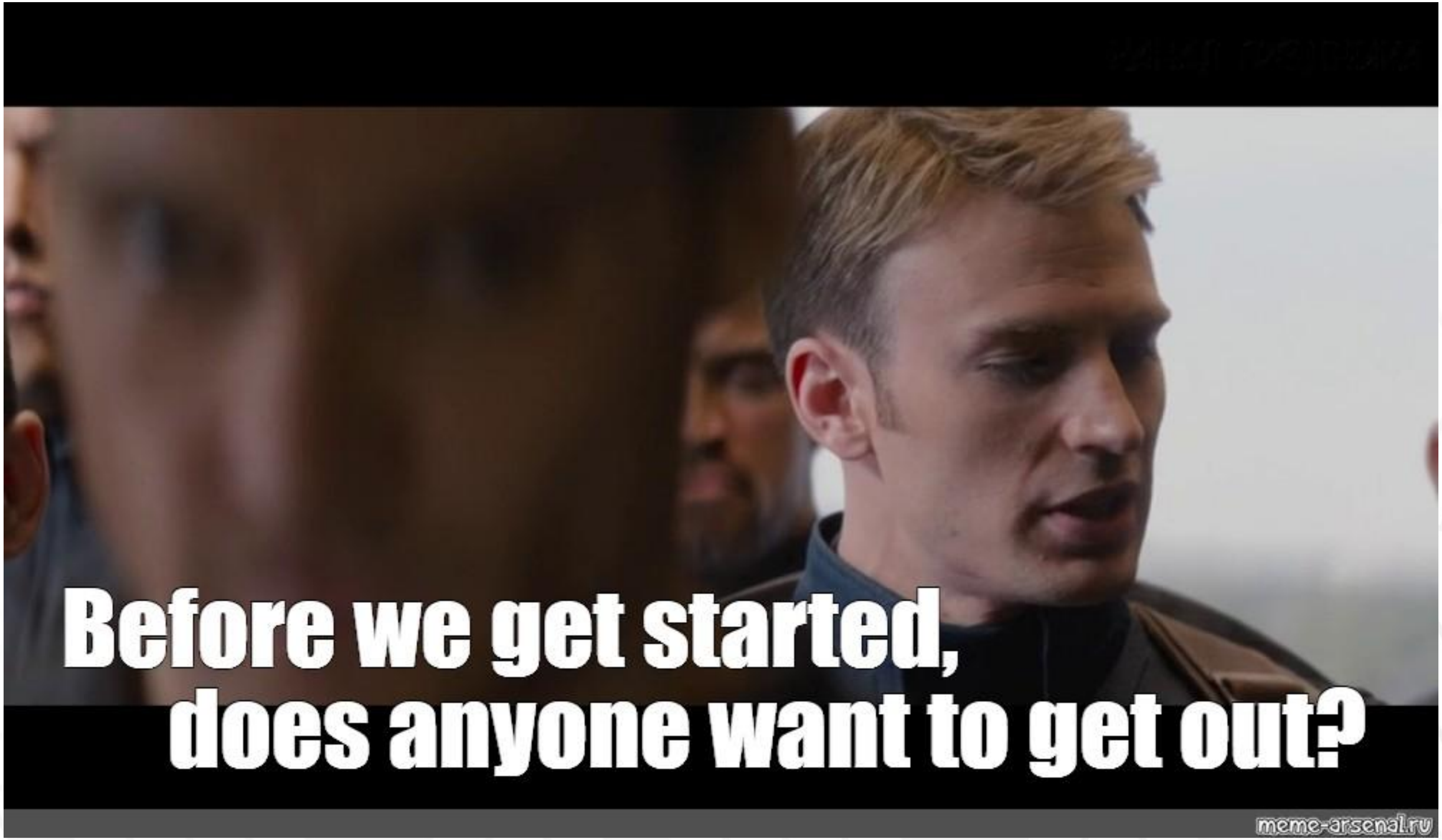
RETHINKING PENETRATION TESTING

REDSIEGE
INFORMATION SECURITY

WHO IS MIKE SAUNDERS

Principal Security Consultant

- 25 Years Experience
  - Penetration Testing
  - Red Teaming
  - IT and Security Expertise
  - System Admin
  - Network Admin
  - Blue Team
  - Development
  - Security Architecture
- Tool Developer
- Technical Blog Writer
- Black Hat Trainer
- Photographer, Musician, Hiker


Before we get started,
does anyone want to get out?
meme-arsenal.ru

WHY AM I HERE?
imgflip.com

Pen Testing is BROKEN

- Traditional network pen tests don't represent how attackers operate
  - Start with host inside the network
  - Focused on coverage vs. depth
  - Noisy scans
  - Most attackers already have credentials (phishing/code execution)
- On the positive side – most likely to identify missing patches

A Better Way?

- Simulate how real attackers might operate
    - Assumed Breach
    - Purple Teams
    - Red Teams

So…Many…Terms…

Pivot

Purple Team

Assumed Breach

Adversarial Attack Simulation

Threat Modeling

Adversary Simulation

Threat Emulation

Attack Simulation

Red Team

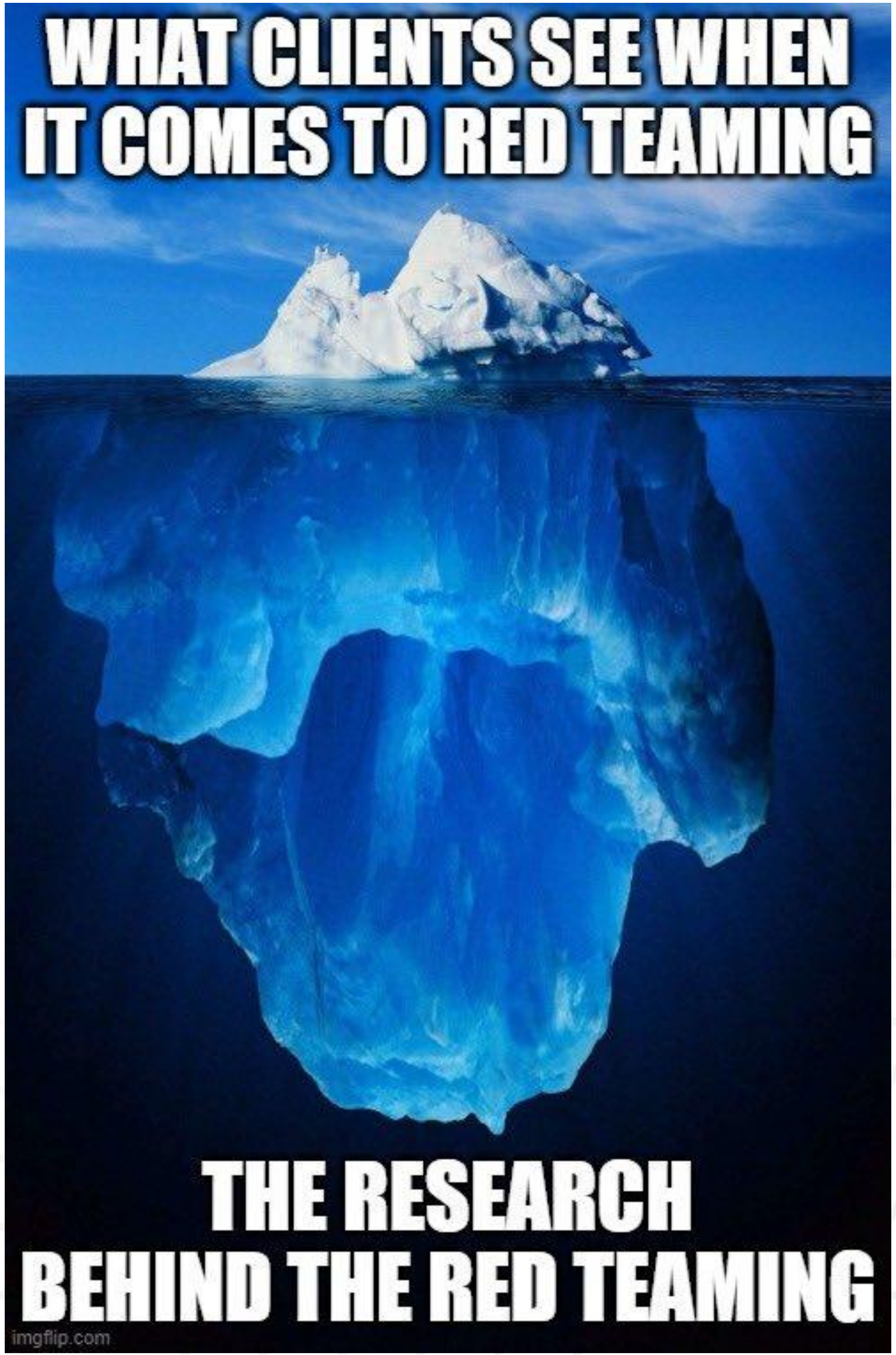
Comprehensive Testing

Red Team Terms

- Attack Simulation
- Adversarial Attack Simulation
- Threat Emulation
- Red Team
- Comprehensive Testing

Red Team?

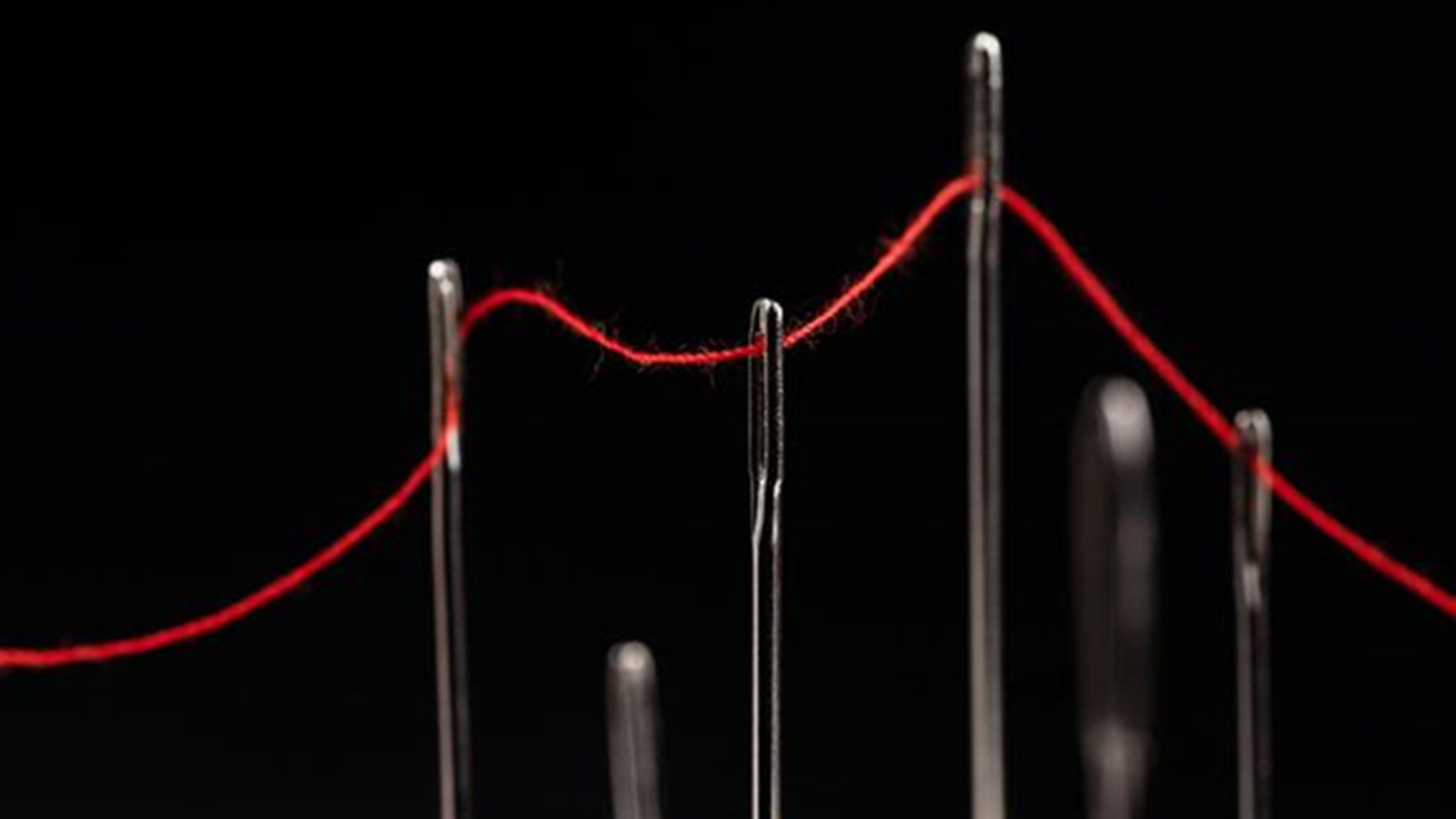
- Emulate an advanced threat actor
  - Phishing / Vishing / Smishing
- Attempt to evade detection
- Establish persistence, lateral movement, privesc
- Usually goal focused
- Long campaigns – typically 6+ weeks
- Tests defenders, not detections


WHAT CLIENTS SEE WHEN IT COMES TO RED TEAMING
THE RESEARCH BEHIND THE RED TEAMING
imgflip.com

@ZephrFish

Pros & Cons: Red Team

- Pro
  - Better understanding of resilience against determined attacker
  - Ability to model real-world TTPs
- Con
  - Expensive
    - Campaigns are long 6+ weeks
    - Requires R&D time for payload and ruse development
  - Attackers have unlimited time, we don't



Pros & Cons: Red Team

- More Con
  - Red Teams aren't threading a needle. They're threading multiple.
    - Protecting infrastructure (Netcraft, etc.)
    - Email filters (M365, ProofPoint, etc.)
    - Getting the right ruse to the right user on the right day
    - Code execution
    - Establishing persistence
    - Staying hidden
- Requires significant maturity to realize value

Assumed Breach

- Assume an endpoint is already compromised & org is breached
- Zero or full knowledge
- Starts on typical end user workstation or with remote access
  - What data can an attacker access?
  - What systems can an attacker access?

Assumed Breach Goals

- Focus on coverage = overt testing
  - No attempts to evade
- Focus on testing detections = covert testing
  - What do security systems see and alert on?

Pros & Cons: AB

- Pro
  - Better understanding of strengths and weaknesses
  - Ability to model real-world TTPs
- Con
  - Limited time = faster tempo, more noise
  - Not focused on vulnerabilities
  - Non-representative accounts/workstations can negatively impact results

Purple Team

- Sometimes threat emulation – emulate a specific attacker, or specific agreed upon techniques
- Highly-collaborative test between blue and red teams -> Purple
- Focused on specific objectives / goals
  - Test assumptions
  - Validate detections & security investment
  - Identify visibility gaps
  - Identify gaps in processes

Pros & Cons: Purple

- Pro
  - Confirm detections and defenses
  - Confirm attack visibility
  - Collaborative & reactive
- Con
  - Not focused on vulnerabilities
  - Not necessarily focused on extent of ability to spread/escalate
  - Blue team may need to respond to actual incidents

A Better Way

AB – TWO(ish) MODELS

- Compromised user
- Malicious user (insider threat)
- Both use standard workstation image with representative user accounts
  - Preferably a recently terminated user & their workstation
  - Backup option – user cloned from active user, machine from gold image

Compromised USER – PATH A

- Simulate a user who executed on a custom payload
- Ops take place over C2 framework
  - Can execute with remote access or ship payload to client
  - Pivot to remote access with creds

Compromised USER – PATH B

- Operate on workstation
  - Shipped laptop / VPN + RDP / on site
- Work with tools available on desktop or what can be loaded
  - Initiate C2 if needed

AV/EDR – DISABLED?

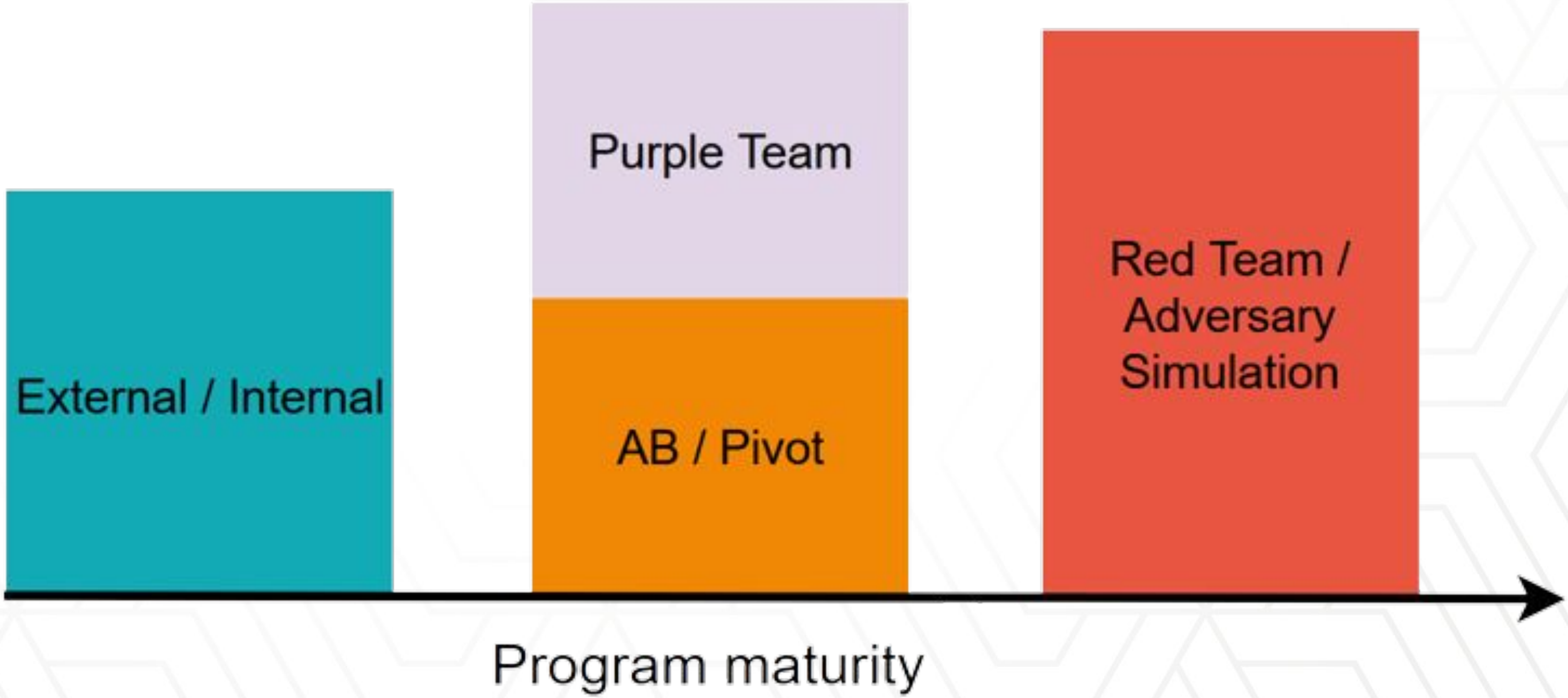
- Any AV/EDR can be bypassed given time
- Is it worth client $$$ to spend time to develop bypass?
- Discuss goals with client
- @HackingLZ – Start with AV/EDR enabled, verify bypass or visibility of actions, then disable if needed
    - Have this discussion before the test starts
    - If protections will be disabled, where and when

It's Time to Buy

REDSIEGE
INFORMATION SECURITY

INITIAL CONTACT & SCOPE

- What are your goals?
  - Test detections and controls
  - Identify misconfigurations
  - Identify vulnerabilities
  - What can an attacker access
  - Can we detect lateral movement
  - Compliance checkmark
- What is your budget?
- How much time / how many resources can you dedicate?



External / Internal

Purple Team

AB / Pivot

Red Team / Adversary Simulation

Program maturity

Tell me the truth...I'm...I'm ready to hear it.
YOU DON'T NEED A RED TEAM ASSESSMENT. YOU NEED TO MASTER THE BASICS.

Questions?

- mike@redsiege.com
- @hardwaterhacker / @redsiege
- https://www.linkedin.com/in/mike-saunders-7902631/
- https://redsiege.com/discord
- https://redsiege.com/wednesday-offensive/

- Slides: https://redsiege.com/rethink

REDSIEGE

INFORMATION SECURITY

BUSINESS:

GETOFFENSIVE@REDSIEGE.COM

OFFENSIVE SERVICES. OFFENSIVE MINDS

- ASSUMED BREACH ASSESSMENT
- PENETRATION TESTING
- WEB APPLICATION PENETRATION TESTING
- RANSOMWARE READINESS ASSESSMENT
- RED TEAM & ADVERSARY EMULATION
- PURPLE TEAM & TRAINING

OUR OFFENSE PREPARES YOUR DEFENSE