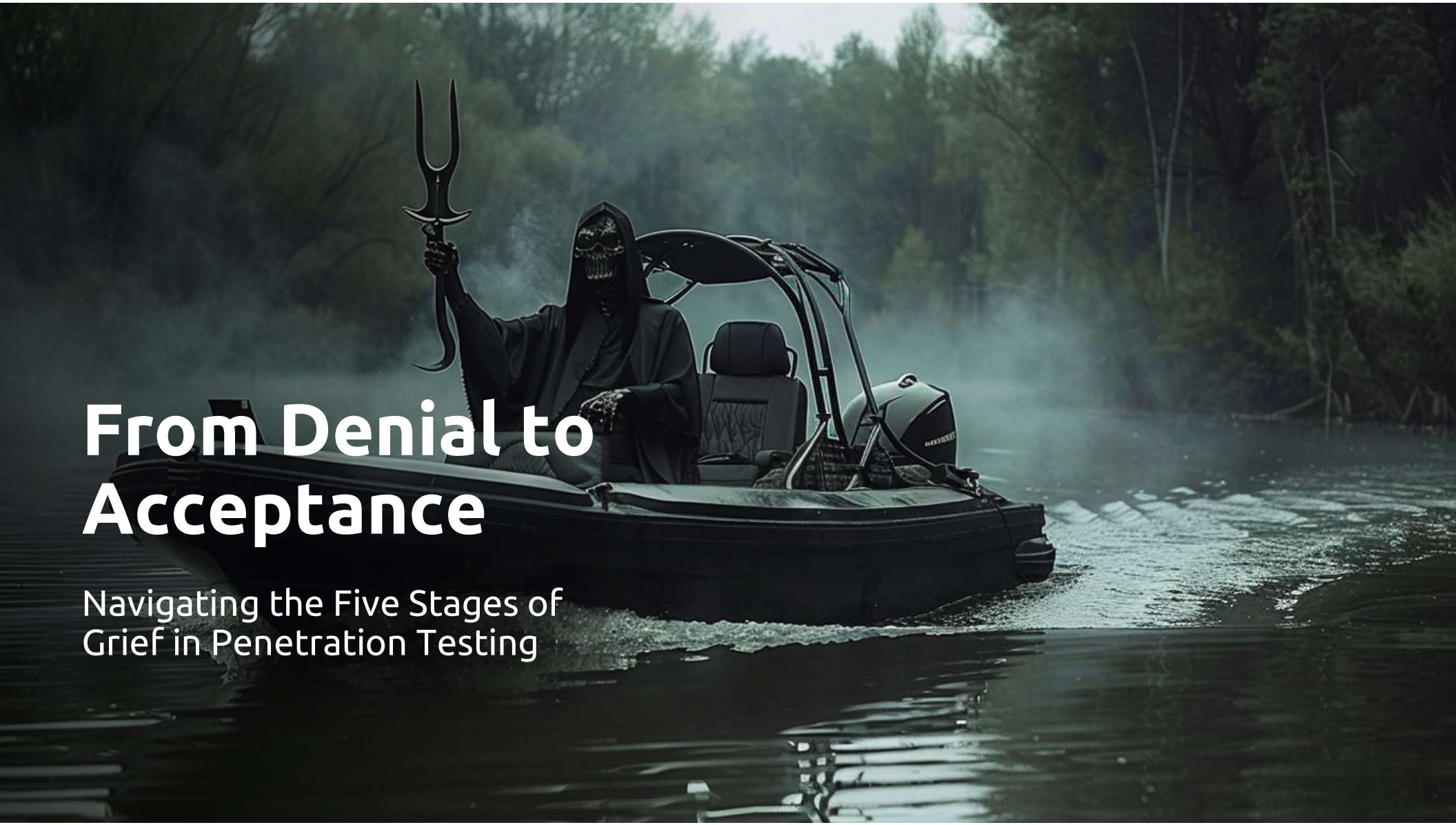


From Denial to Acceptance

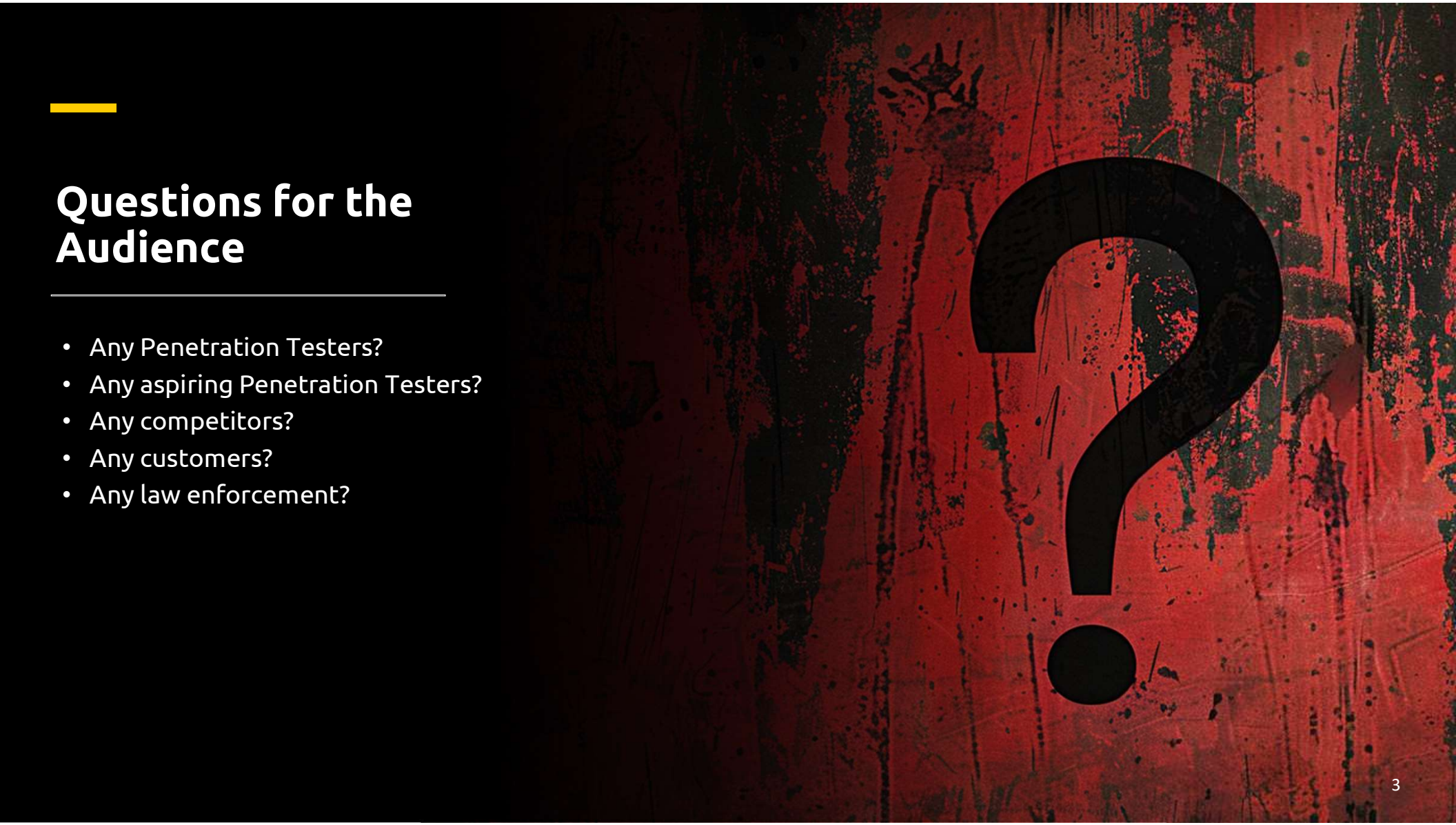
Navigating the Five Stages of Grief in Penetration Testing

Disclaimer

- Opinions and statements made in this presentation are not the opinions or statements of SynerComm
- The opinions and statements made in this presentation are the opinions and statements of the presenter only.
- None of the information is legal, financial, or health care advice

Questions for the Audience

- Any Penetration Testers?
- Any aspiring Penetration Testers?
- Any competitors?
- Any customers?
- Any law enforcement?



Who Are You and What Are You Doing in My Computer?

- Ryan Zagrodnik, OSCP, CISSP
  - Legal Criminal, 5.5 years with SynerComm, external/internal, wireless, web app, and physical penetration tests
  - 22 long years in the Cybers (Aging like a President)
  - Began as an overworked-crushed-soul (SysAdmin)
  - Big Dater, Finance, Health, gubmint contracting, industries
  - Cofounder: Madison, WI DEF CON Group https://dc608.org 501(c)(3)
  - @TheL0singEdge
  - Husband
  - Rescuer of cats and dog
  - Pontoon boat captain
  - Commercial airline pilot (virtual and drone)
  - I used to be cool (was young, fit, had a CBR & Harley)

SYNERCOMM

Why Are You Doing This?

- Inspire and motivate
  - You're only a loser if you stop trying
- I actually want to give this talk
- Practice for my standup comedy career
- SynerComm supports the community by giving away content
- Provide advice based on the last 20 years of my life
- Nobody gives talks on their failures
- There is a lot of similarities with grief and penetration testing
- Stuff I wished I knew
- Mostly humble bragging

What are the Five Stages of Grief?

1. **Denial:** Refusal to accept the reality of the situation.
2. **Anger:** Frustration and anger over the situation.
3. **Bargaining:** Attempting to negotiate or make deals to change the situation.
4. **Depression:** Deep sadness and despair about the situation.
5. **Acceptance:** Coming to terms with the reality of the situation and moving forward

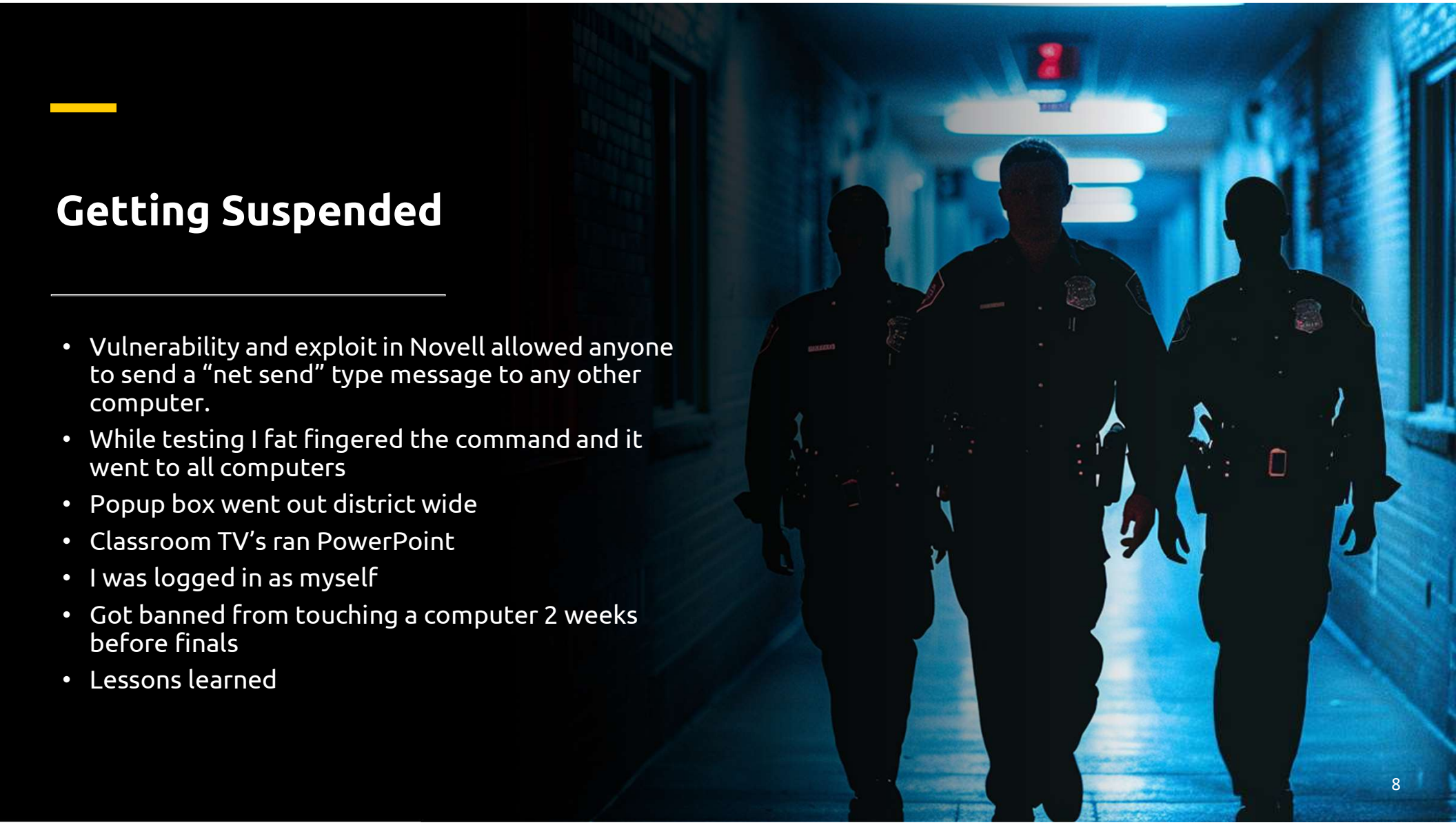
SYNERCOMM

Why Grief?

- What are you some kind of emo?
  - No.
    - I have been through loss of life.
    - If you haven't yet, get ready because the great equalizer is coming for you.
    - Goth's are people too.
- You go through grief more than you know.
  - Grief is not limited to the loss of life.
    - **Divorce or Breakups:** Individuals may experience denial, anger, bargaining, depression, and acceptance as they come to terms with the end of a relationship.
    - **Job Loss:** Losing a job can trigger the same stages as one processes the shock, frustration, attempts to regain the position, sadness, and eventual acceptance of moving forward.
    - **Health Issues:** A diagnosis of a serious illness or chronic condition can lead individuals through these stages as they adjust to their new reality.
    - **Major Life Changes:** Events like moving to a new city, retiring, or significant lifestyle changes can also invoke the stages of grief as one adapts to new circumstances.
    - **Financial Loss:** Experiencing a significant financial setback, such as bankruptcy, can lead to grieving over the loss of financial stability and future plans.

Getting Suspended

- Vulnerability and exploit in Novell allowed anyone to send a “net send” type message to any other computer.
- While testing I fat fingered the command and it went to all computers
- Popup box went out district wide
- Classroom TV’s ran PowerPoint
- I was logged in as myself
- Got banned from touching a computer 2 weeks before finals
- Lessons learned



Offensive Security Certified Professional (OSCP)

The OSCP (Offensive Security Certified Professional) exam is a well-regarded certification in the field of cybersecurity. It is administered by Offensive Security and focuses on practical, hands-on skills in penetration testing. The exam involves:

1. **24-Hour Lab-Based Test**: Candidates are given 24 hours to complete a series of penetration tests on various machines within a controlled environment.

2. **Report Writing**: After completing the lab portion, candidates must submit a comprehensive report detailing their findings, methodologies, and any exploited vulnerabilities.

The OSCP certification is known for its rigorous nature and emphasis on practical, real-world hacking skills, making it a prestigious credential for security professionals.

Why Do Employers Like the OSCP?

1. Practical Skills: The OSCP emphasizes hands-on, real-world penetration testing skills. This ensures that certified individuals can effectively identify and exploit vulnerabilities in a network, which is crucial for cybersecurity roles.

2. Problem-Solving Ability: The 24-hour practical exam tests candidates' ability to think critically and solve complex problems under pressure, a valuable skill in cybersecurity.

3. Technical Proficiency: Passing the OSCP demonstrates a high level of technical knowledge and expertise in areas such as network security, exploitation, and various attack methodologies.

4. Commitment and Dedication: The rigorous nature of the exam requires significant preparation and persistence, indicating a candidate's dedication and determination to excel in the field of cybersecurity.

5. Industry Recognition: The OSCP is well-respected within the cybersecurity community and is often considered a benchmark for penetration testing skills, making certified professionals more attractive to employers.

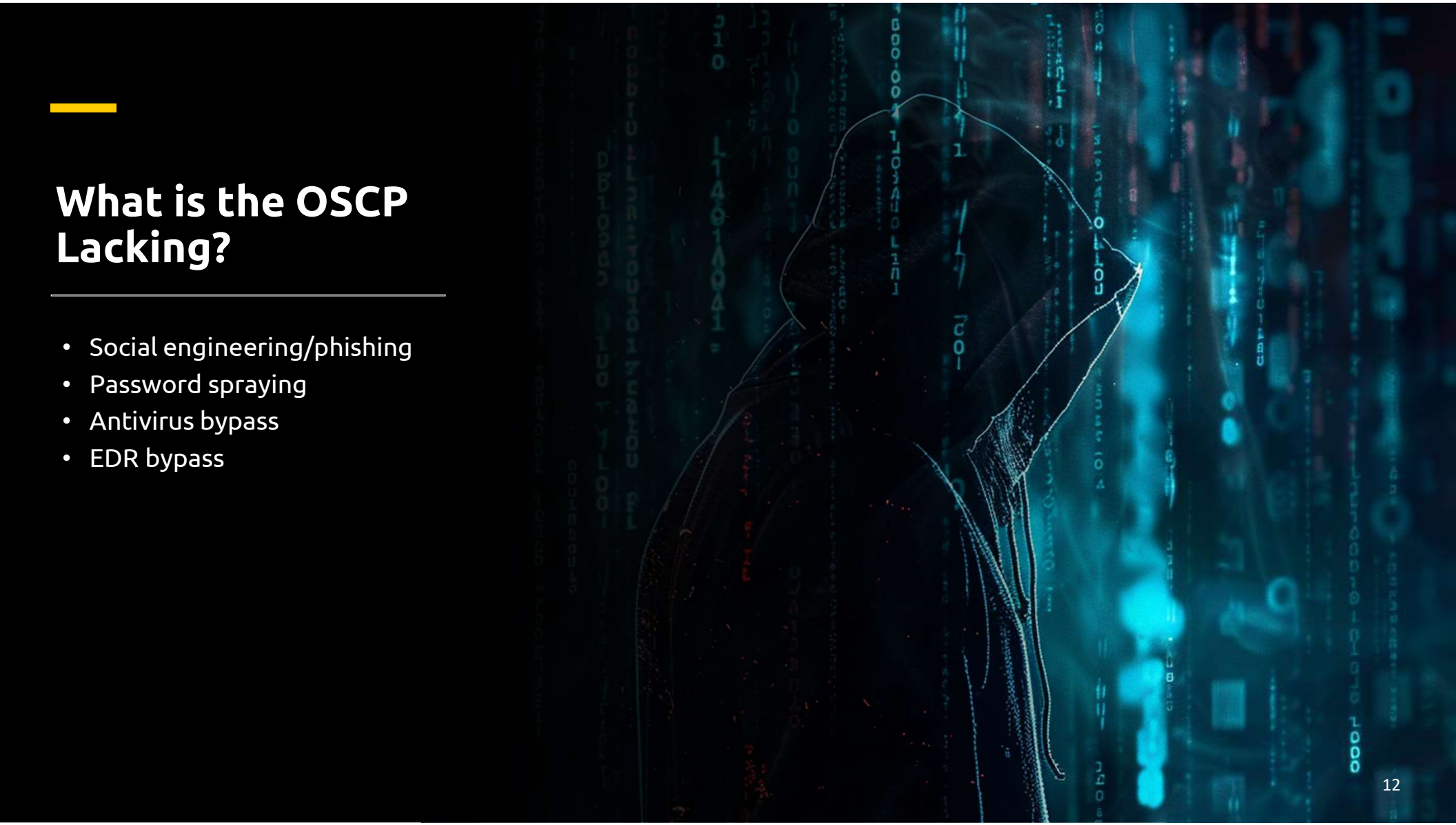
Why Do Employers Really Like The OSCP?

- The grinding.

- The new version of the OSCP is more real life; however, it's still a Capture the Flag (CTF) exam IMO.

What is the OSCP Lacking?

- Social engineering/phishing
- Password spraying
- Antivirus bypass
- EDR bypass



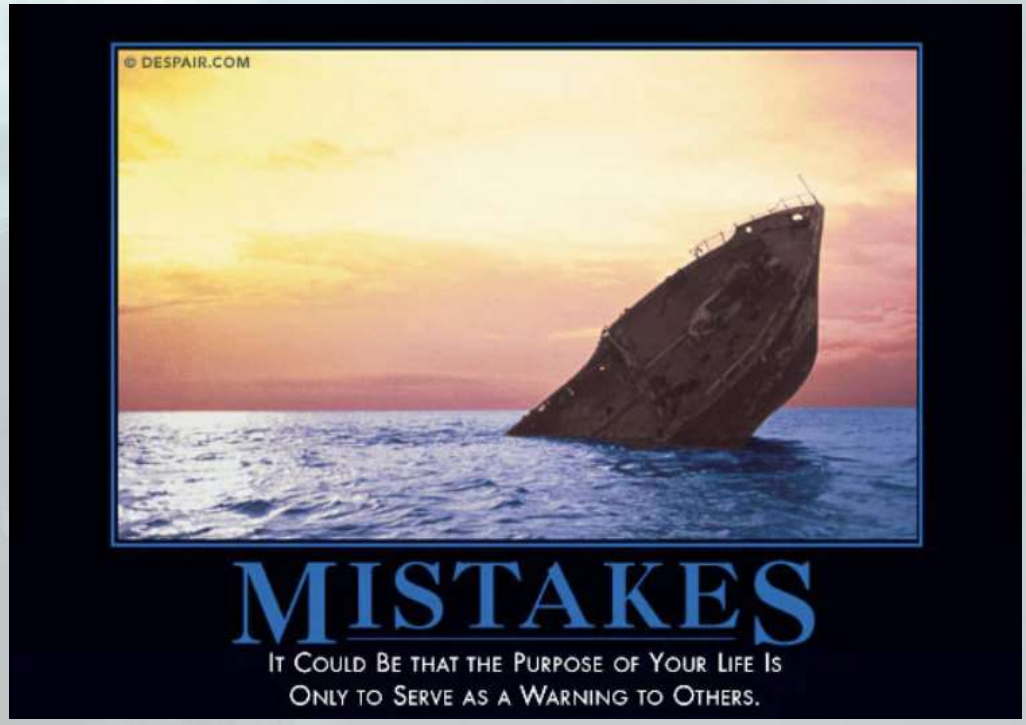
My OSCP Exam Experience(s)

- I set a goal to become penetration tester as a consultant in 2012.
- I took the OSCP exam for the first time in 2013 when it was still Penetration Testing with Backtrack.
- I took the exam several more times between then and 2023.
- Closest attempt 65 out of the 70 points.
  - Buffer Overflow (25 points).
  - The 10-pointer.
  - Low privilege shell 20-pointer (10 points)
  - Low privilege shell 20-pointer (10 points)
  - Bonus points rooted and documented lab systems (10 points)
  - The next 12 hours of despair and no sleep
    - All stages of grief
      - Denial
      - Anger
      - Bargaining
      - Depression
      - Acceptance
- Failure. Total points 65.

SYNERCOMM

How To Avoid My (Many) Mistakes

- Time Management
  - You're not supposed to stay awake for the full 24 hours.
- Energy drinks
  - There is such a thing as too much energy.
- Breaks
  - Your brain will continue to work on the problem without you being aware of it.
- Mindset
  - IMO the best mindset is to set your expectations to experience the exam. Not to pass it.
  - Be at peace with the outcome beforehand
- Synthwave



SYNERCOMM

My Advice / Teach Me to Hack

- TryHackMe
- TJNulls List
  - Google: “TJ Null list got updated site:reddit.com”
- Hack the Box (HTB)
  - https://www.hackthebox.com/
- Python3
  - Udemy, Code Academy, PluralSite, Leetcode, etc.
- IppSec’s YouTube Channel
- Offsec’s Proving Grounds
  - Play (free)
  - Practice ($19)
- Offsec’s Learn One ($2,499)
- Offsec’s 90 Days package ($1349)
- Invoke the muses (Book: Put Your Ass Where Your Heart Wants to Be)
- Take care of yourself

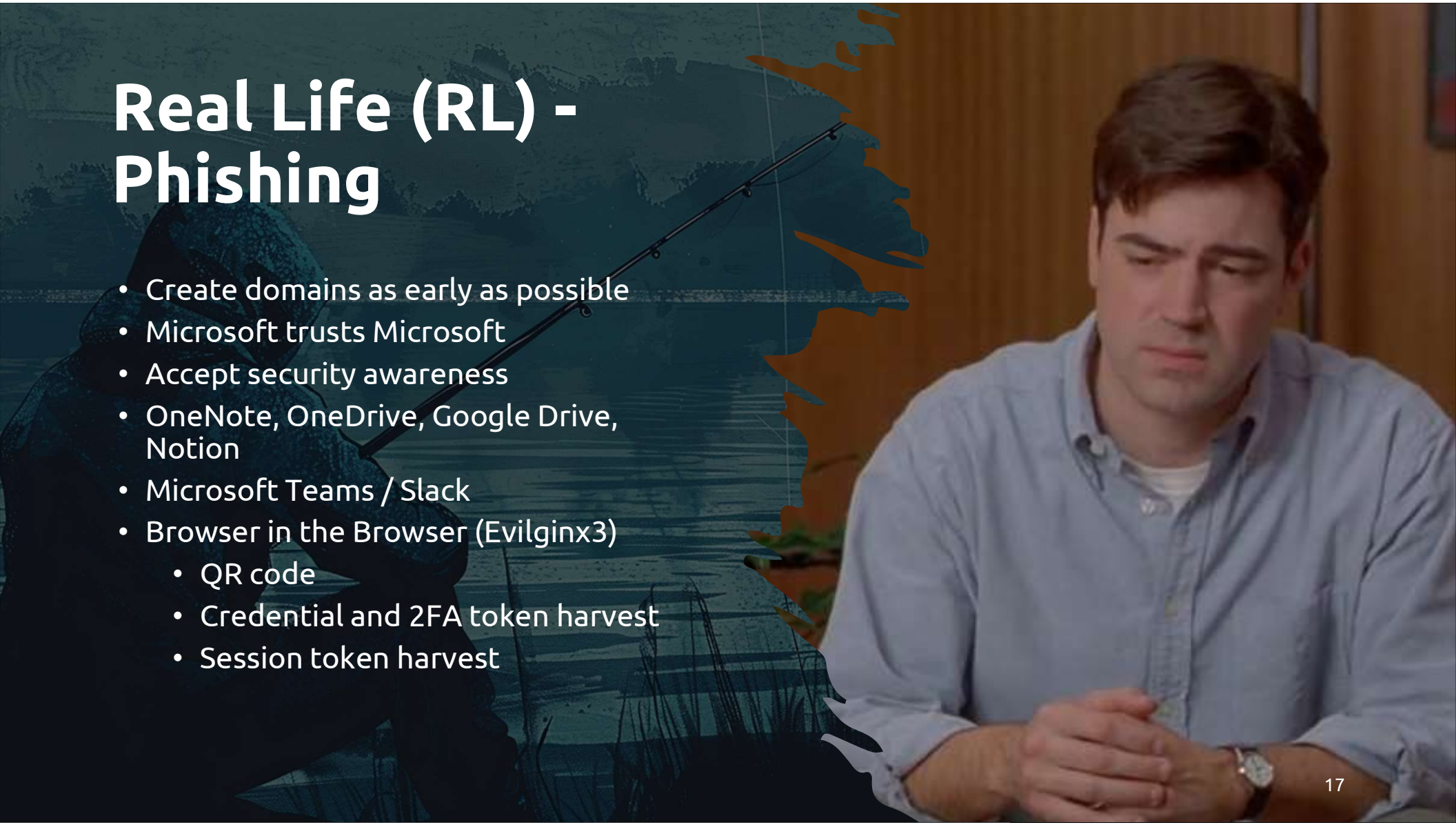
SYNERCOMM

Real Life (RL) – External Penetration Tests

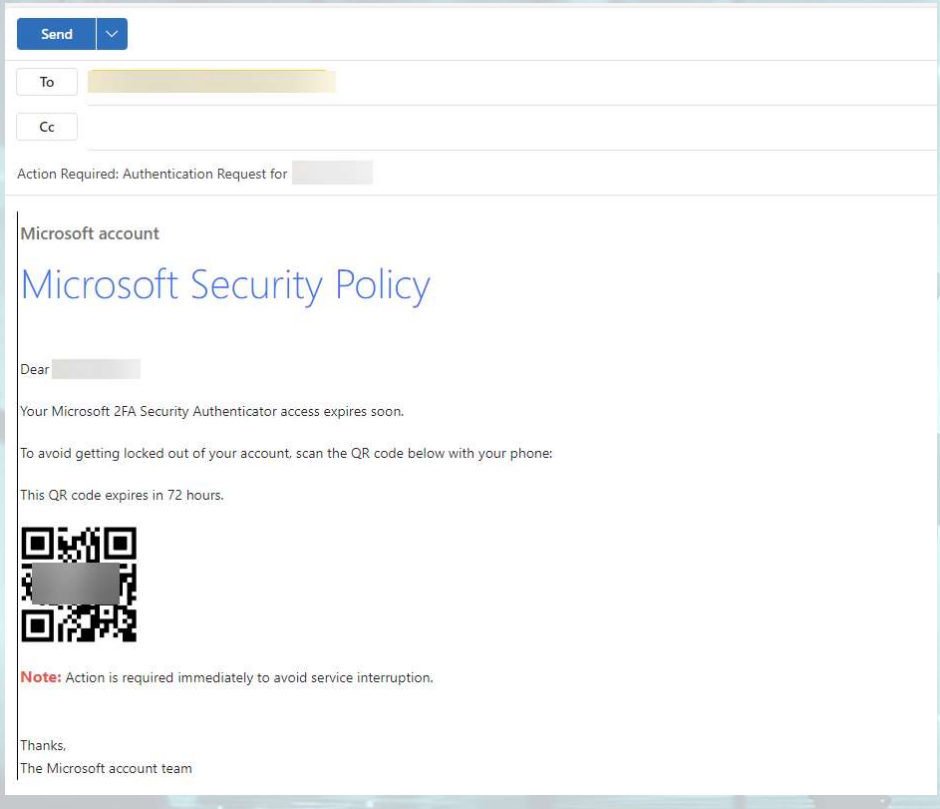
- C2 tradecraft
  - Domain fronting and categorized domains
  - Binary
  - Macros bro
  - Embed raw Cobalt Strike payload
  - Obfuscate with Shellter pro
  - Sign with EV code signing certificate
  - Test – gets eaten by Palo Alto
- Password spraying and social engineering is our bread and butter
  - If you don't allow these on an engagement, you are doing yourself a disservice
- 0-days are rare, but they are there
- Outdated web apps are king
- Acceptance
  - External penetration tests are hard
  - Scope and time is limited

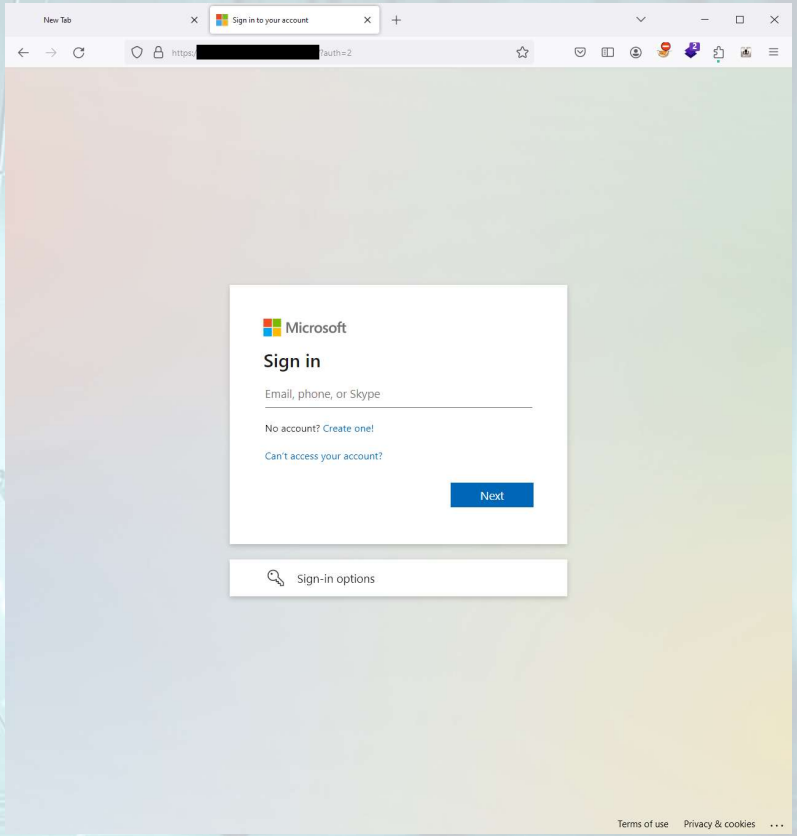
Real Life (RL) - Phishing

- Create domains as early as possible
- Microsoft trusts Microsoft
- Accept security awareness
- OneNote, OneDrive, Google Drive, Notion
- Microsoft Teams / Slack
- Browser in the Browser (Evilginx3)
  - QR code
  - Credential and 2FA token harvest
  - Session token harvest



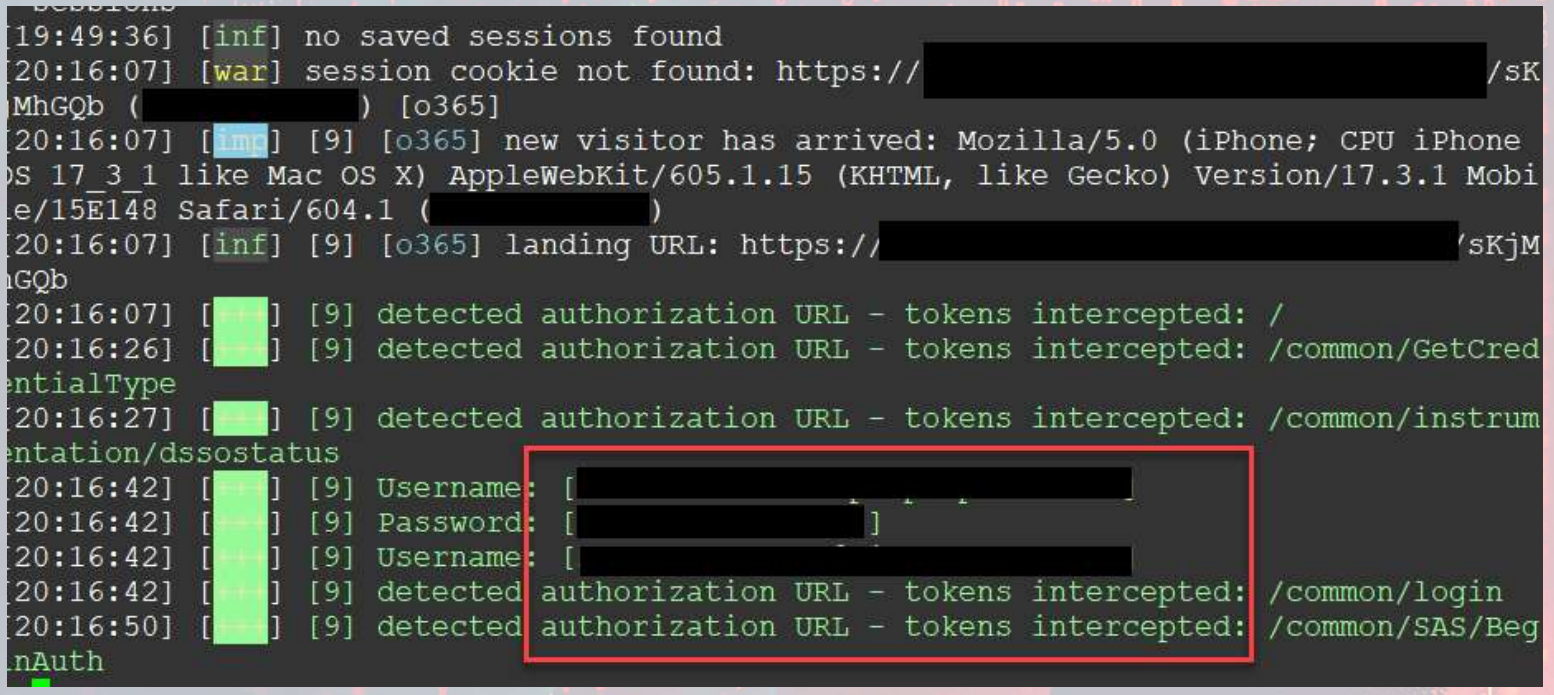
Real Life (RL) – Phishing - Continued





SYNERCOMM

Owned



SYNERCOMM

Owned - Continued

[redacted] [Phish Alert] [EXTERNAL] Action Required: Authentication Request for [redacted]

[redacted] [redacted]

To: [redacted]

Reply | Reply all | Forward

Wed 2/28/2024 2:42 PM

I did scan the QR code that was in the email on my work phone and unfortunately entered my email/password. I've gotten so many authenticating things lately with just starting I figured it was another one until I asked someone by me.

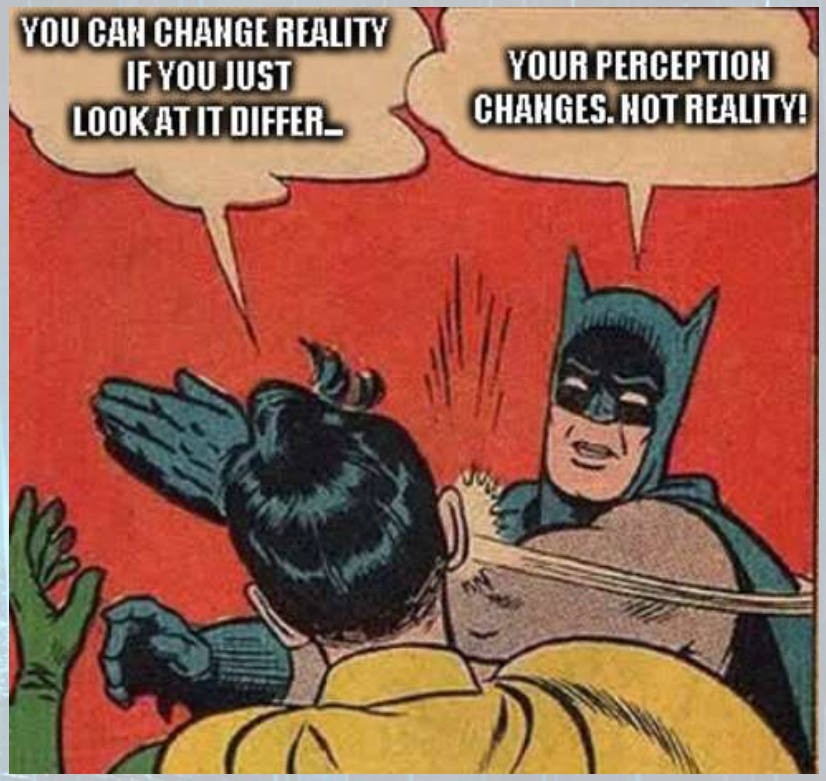
...

Reply | Forward

SYNERCOMM

Real Life (RL) – Internal Penetration Tests

- I don’t always get Domain Admin
  - I hate losing
- Change your perception
  - Not you vs the org
  - Point in time engagement
  - Stick to the facts
  - The engagement is a partnership
  - The org is winning because it’s better we find it than ransomware



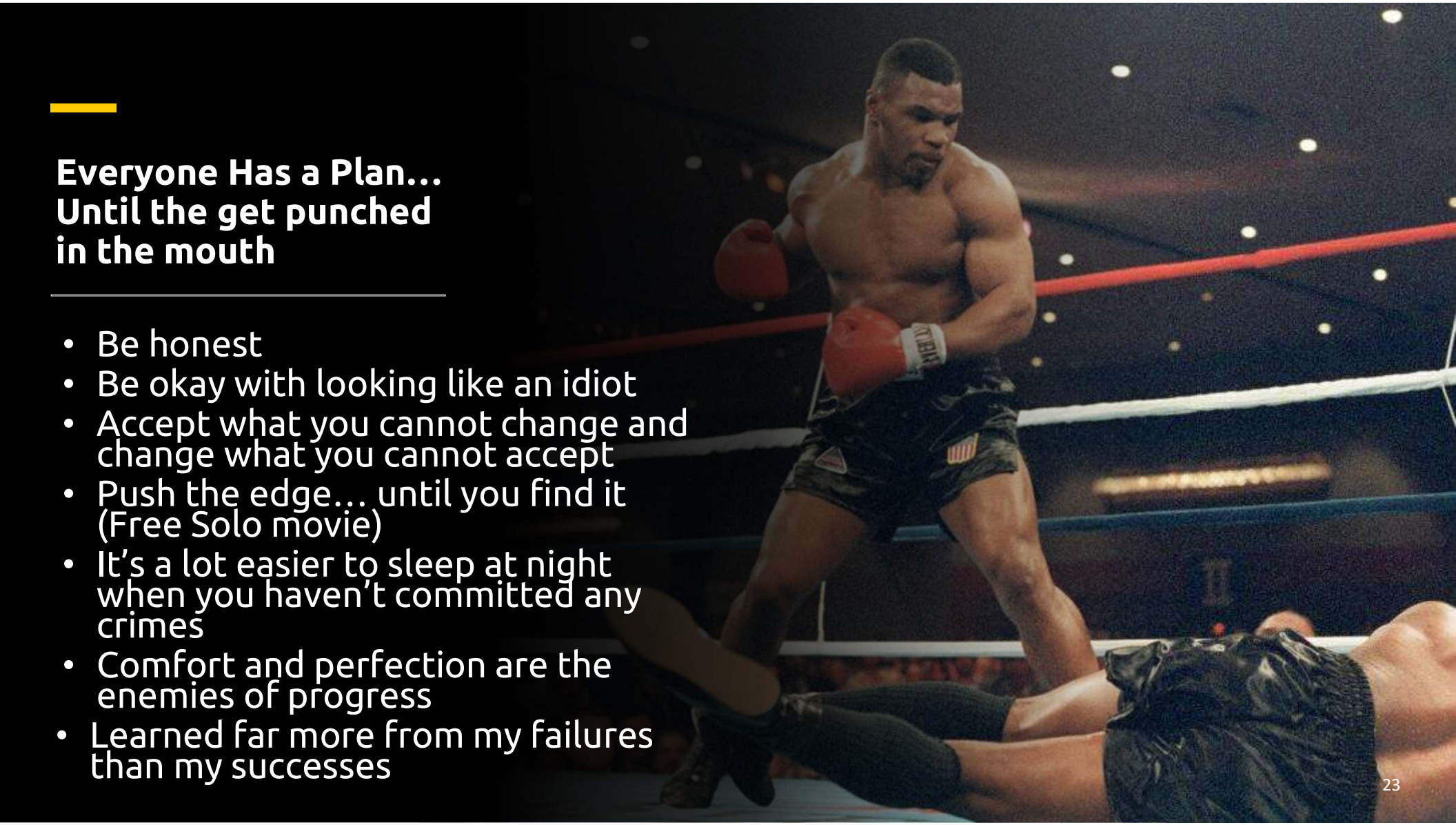
SYNERCOMM

Real Life (RL) – Physical Penetration Tests

- Fake it until you make it
  - Pretending to be an optimist looks the same as being an optimist
- No way there's social security numbers in this dumpster
  - Surprise there is
- Panic attacks
  - Meditation and breathing exercises (Headspace, Insight Timer, Wim Hof Method)
- Tailgating is king
  - The beep when swiping your work badge does not mean that it was authorized. It means the card was read.
- Ask if the guards are armed
- Guilt
  - Accept that lying to people is good for them (Better us than real life threat)
- Anger
  - Be prepared that some will be less than pleased with your behavior
- Sweat towels

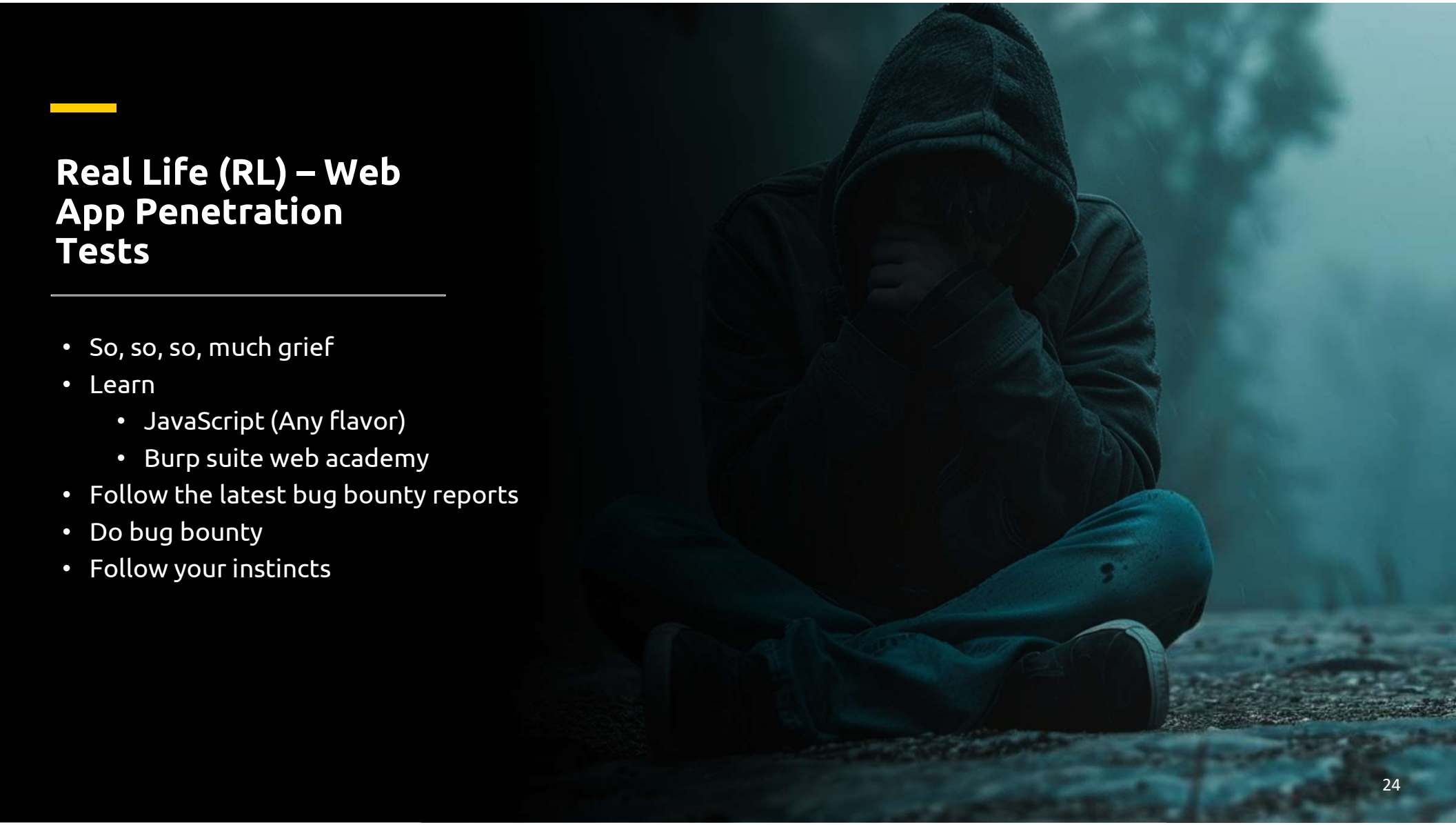
Everyone Has a Plan… Until the get punched in the mouth

- Be honest
- Be okay with looking like an idiot
- Accept what you cannot change and change what you cannot accept
- Push the edge… until you find it (Free Solo movie)
- It’s a lot easier to sleep at night when you haven’t committed any crimes
- Comfort and perfection are the enemies of progress
- Learned far more from my failures than my successes



Real Life (RL) – Web App Penetration Tests

- So, so, so, much grief
- Learn
  - JavaScript (Any flavor)
  - Burp suite web academy
- Follow the latest bug bounty reports
- Do bug bounty
- Follow your instincts



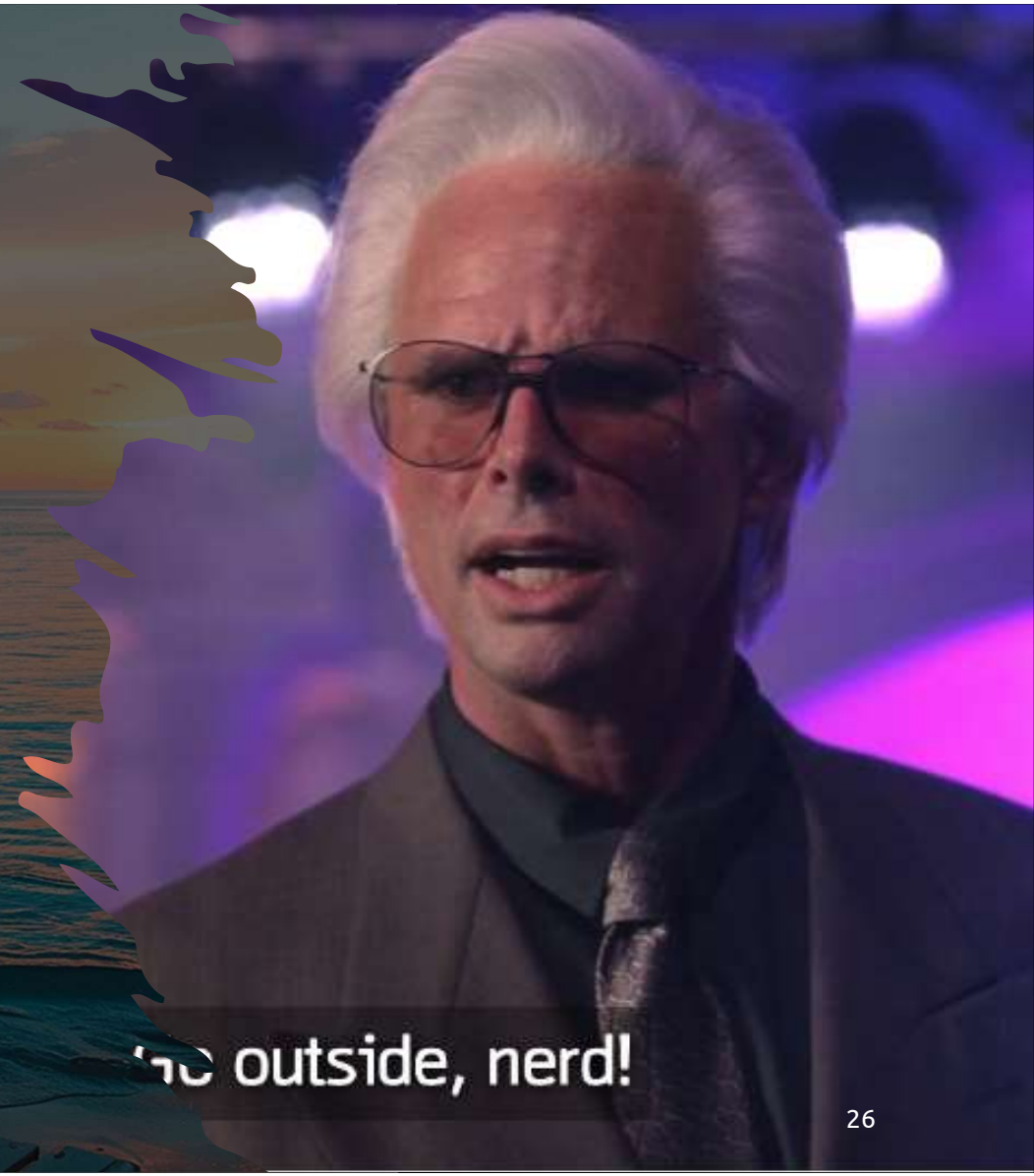
Real Life (RL) – Wireless

- Evil twin
- Password spraying online portals
- 2FA
- WPA handshake
  - 4-step process used in WPA/WPA2 protocols to securely establish a connection between a client and a wireless access point, ensuring both parties have the correct credentials and securely exchanging encryption keys for data transmission.
- Pairwise Master Key Identifier (PMKID)
  - PMKID is a unique identifier used in the process of creating and authenticating the Pairwise Master Key (PMK), which is crucial for establishing a secure connection between a client and an access point in a Wi-Fi network.
  - The PMKID is used during the 4-way handshake process to derive the session keys that encrypt the data transmitted over the wireless network.
- Use WPA3

Real Rest and Relaxation (R&R) - Recharging

- What it isn't:
  - Games where you grind MMORPG, Battle Royals, Rocket League
  - Party rocking

- What it is:
  - Nothing is wasted time if you enjoy it
  - Meditation/Breath work
  - Nature
  - Sleep
  - Nutrition
  - Physical activity
  - Social connections
  - Massage, yoga, tai chi
  - Non player vs player (PVP) games
    - No man's sky
    - Stardew Valley



Tony Robbins

- **Love not hate**
- **Your mood is your fortune**
  - Most people are just reactive..
  - Good weather, good mood. Bad weather, bad mood. No traffic? Good mood. Mean boss? Bad mood.
  - If you can control your mood, you're unstoppable. You're unconditional.
  - Moods are like muscles. The more you do a certain mood (e.g. playful, anxious etc.), the better you are at it.
  - Everybody has times where they are very generous. And times we're assholes
  - But…where do you spend the most time? That's your emotional home.
  - My emotional home before == stressed / anxious
  - My emotional home after == joy & curiosity

Tony Robbins - Continued

What's the fastest way to become more successful…?

- Proximity is Power.
- Surround yourself with people who already are doing that thing.

The difference between a master & a dabbler

- There are 3 types of entrepreneurs.
  - **Dabbler** == tries things, gives up when it gets hard, moves onto the next thing
  - **Stresser Achiever** == they don't give up, but they stress out, grind thru (even take pride in the 'grind' foolishly). They usually achieve success, but don't enjoy the journey, which is a fancy way to fail.
  - **The master** - the master KNOWS and EXPECTS plateaus.
    - When you hit a plateau, the master greets it warmly hello my old friend, I thought you'd be coming soon.
    - They have a strategy for plateaus. They don't get upset. They find other masters to talk to. They slow down temporarily, so they can find a way to the next level.
    - Be a master

SYNERCOMM

Tony Robbins - Continued

This one word equals happiness… what is it?

- People think happiness is this nirvana. Some impossible to reach end state.
- Happiness is simple. Happiness equals progress.
- That's it.

How to get your feet to move in the same direction of your lips

- Confidence is the byproduct of adventure.
- If you want more confidence, just increase the amount of adventure (saying yes to things that are outside your comfort zone).
- Every time you have an adventure, and you don't die, your brain becomes more confident (I can do this, and it's not so bad, next time I won't be afraid)

SYNERCOMM

Books

- The Cuckoo's Egg
- So Good They Can’t Ignore You
- Put Your Ass Where Your Heart Wants to Be
- Die with Zero
- Getting Started in Infosec Consulting
- The Way of the Bull
- How to Keep House While Drowning
- Stolen Focus
- Amusing Ourselves to Death
- Turning Pro
- Four Thousand Weeks
- Digital Minimalism
- Atomic Habits
- Peace is Every Step
- Switch
- The Power of Now
- Meditations

SYNERCOMM

Podcasts

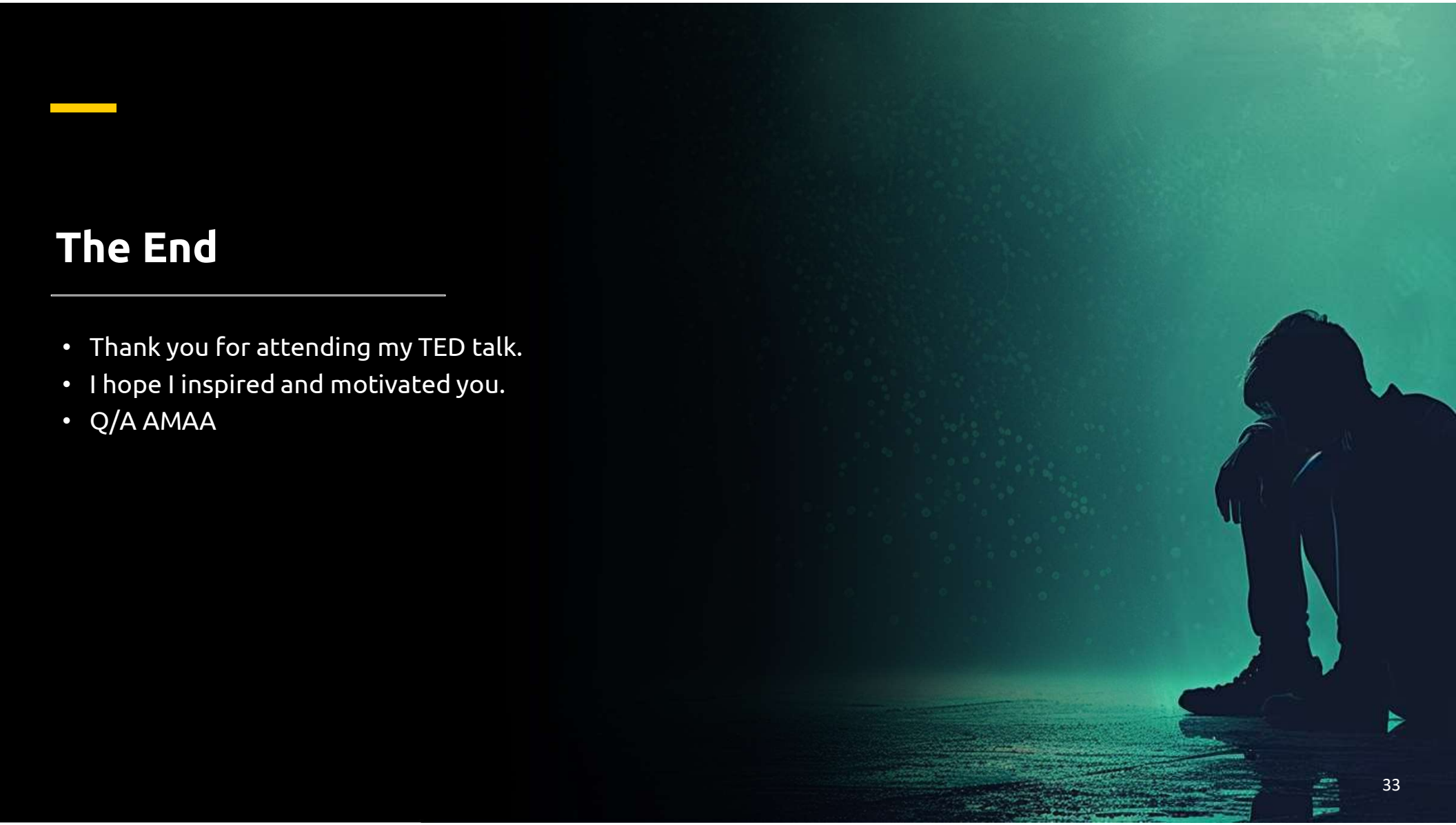
- Unsupervised Learning – Daniel Miesller
- Darknet Diaries – Jack Rhysider
- Risky Business – Patrick Gray
- Critical Thinking – Justin Gardner
-

In Conclusion

- Don’t compare your inside to someone else’s outside
- Instead, compare yourself yesterday to today
- Your old self will remerge
- Little changes will add up to big changes
- Achieving your goals won’t necessarily make you happy
- Loneliness and isolation is good for no one
- Be rare and valuable
- Do the right thing
- None of us is as strong as all of us
- Your actions are your only true possessions
- If don’t have health; you have nothing
- You’re only a loser if you stop trying

The End

- Thank you for attending my TED talk.
- I hope I inspired and motivated you.
- Q/A AMAA



Templates

- Template

SYNERCOMM