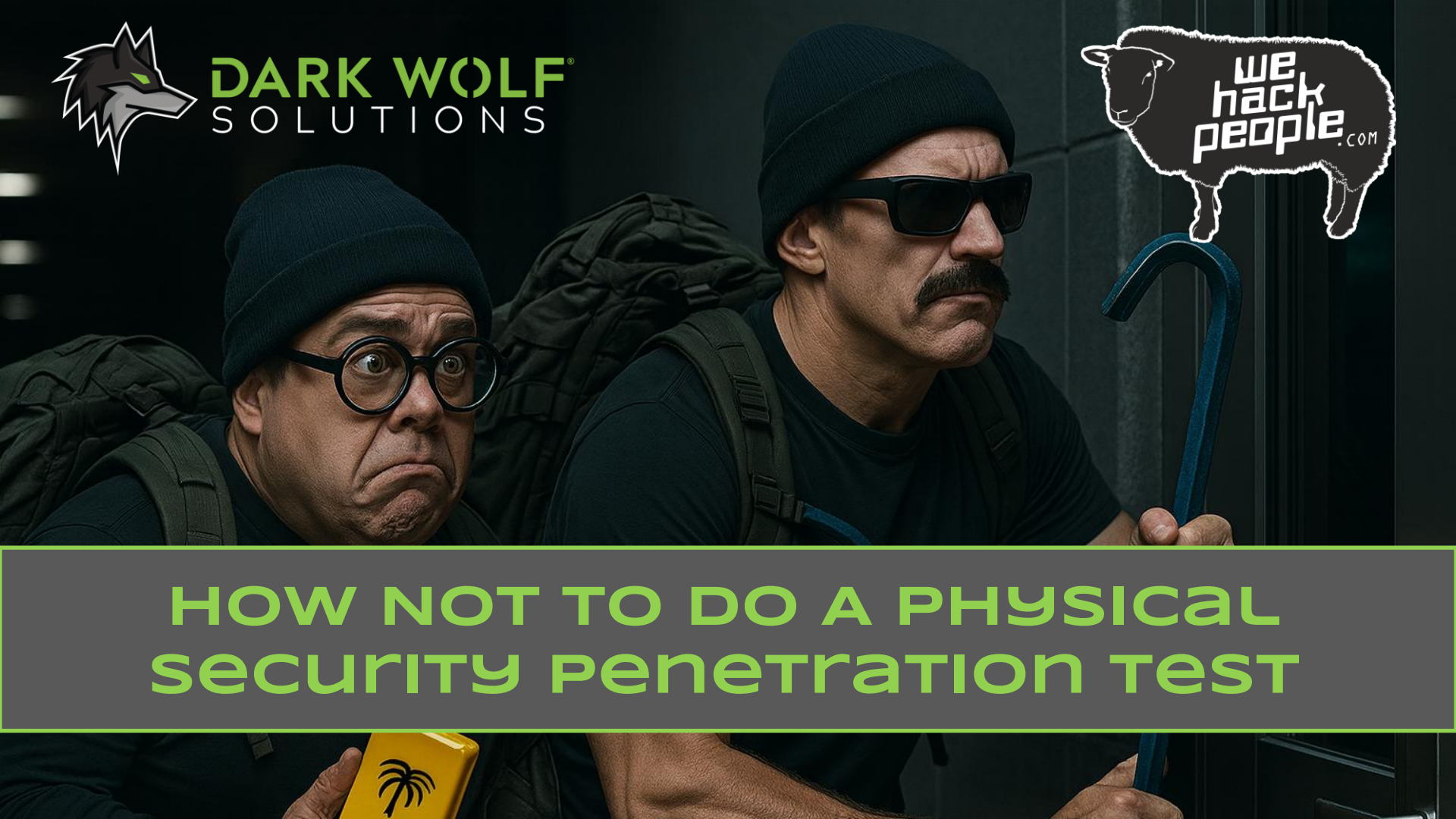

DARK WOLF
SOLUTIONS
we hack people.com
HOW NOT TO DO A PHYSICAL SECURITY PENETRATION TEST

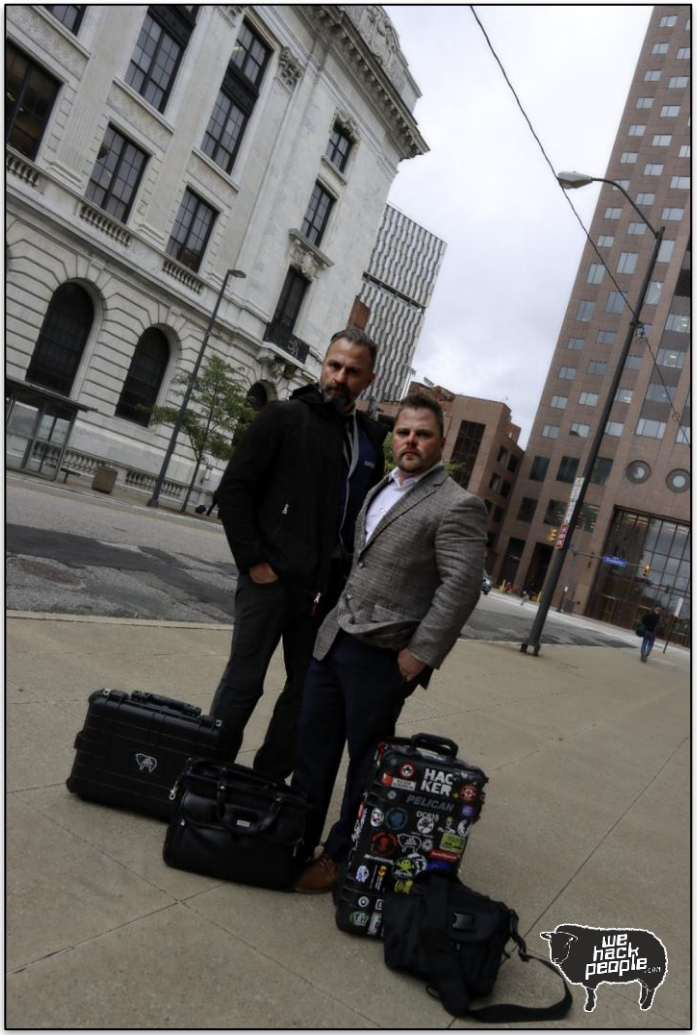
Who are these guys again?

Tim Roberts and Brent White are nationally recognized security professionals, ethical hackers, and the dynamic duo behind WeHackPeople.com. Together, they specialize in social engineering and covert entry, offering real-world insights into how attackers think, operate, and exploit both digital and physical systems.

With decades of combined experience, Tim and Brent have conducted hundreds of Red Team operations across high-risk industries, simulating advanced adversaries to expose critical security flaws. Their work includes breaking into data centers, implanting rogue devices, cloning access badges, and bypassing high-security environments - all while documenting their findings to help organizations improve their defenses.

Tim and Brent have been featured in Profiling Evil, CSO Online, HelpNetSecurity, and Roadtrip Nation and are frequent speakers/trainers at DEF CON, Black Hat, and several industry conferences.

Whether training teams on awareness or keynoting on the human element of security, Tim and Brent are known for their candid storytelling, practical expertise, and engaging presentations that challenge audiences to rethink what “secure” really means.



overview

Even seasoned covert entry specialists can make mistakes…

We'll focus on how NOT to perform covert entry assessments, addressing failures, Hollywood myths, ethical boundaries, and tactical errors that can put clients, reputations, and personal safety at risk.

You will learn practical approaches to avoid these mistakes while still delivering consistent, reliable, and professional results. Let's talk and no death by PowerPoint!

- **No question is stupid!**
- **We can all learn from each other.**
- **We highly encourage questions throughout the presentation.**



Introduction: The Mission

> Reminder:
Primary goal = Identify vulnerabilities, *without* causing damage to property, reputation, or people.

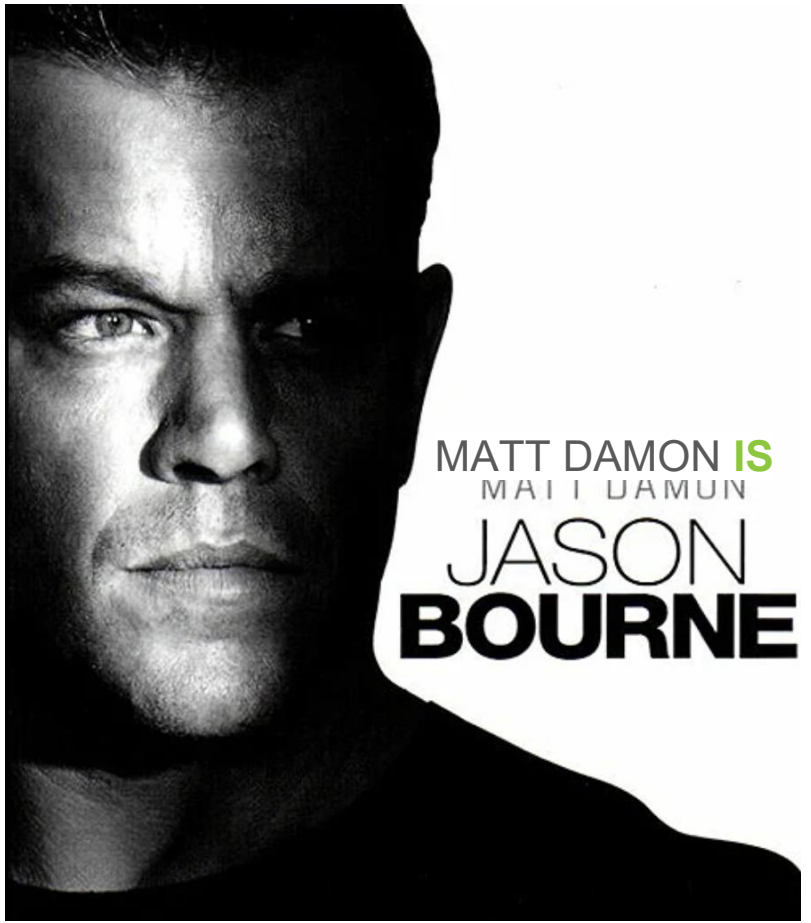
- **Be Forgettable, Not Famous:** You are there to help, not over-hype.
- **Protect the Client's Trust:** Always remember you represent your business, the client, and not just yourself.
- **Stay Professional, Stay Safe:** Reputation takes years to build, seconds to lose.
- **Understand Your Client's Goals:** Know why you're doing this and what success looks like.



HOLLYWOOD MYTH VS REALITY

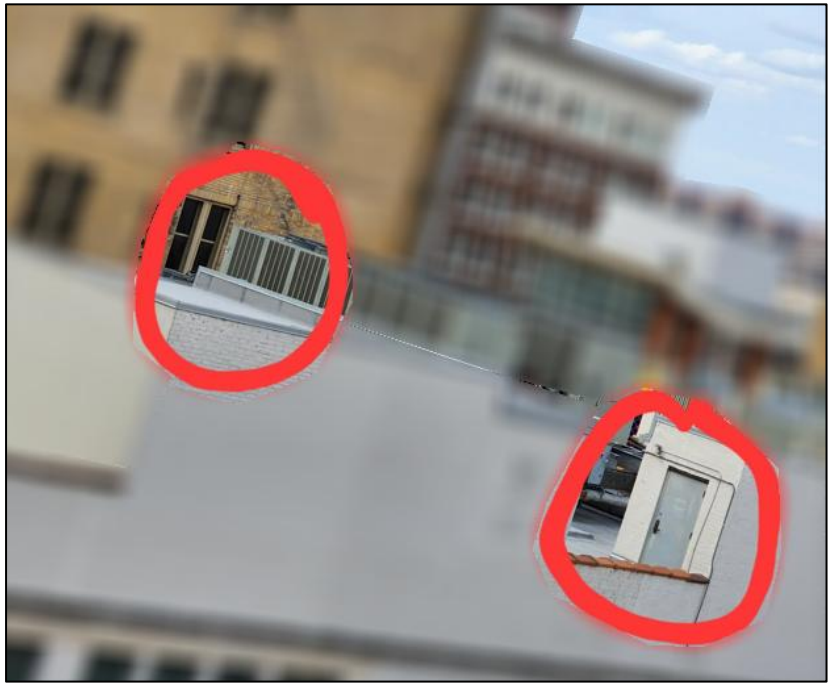
YOU ARE NOT Jason Bourne:

- No martial arts fights with security.
- No rooftop chases.
- No rooftop grappling hooks



HOLLYWOOD: MYTHS VS REALITY

Rooftop entrances can be simple and quiet
with proper reconnaissance and preparation.





HOLLYWOOD: MYTHS VS REALITY

Not Every Bypass is a 5-Second Click

Set Realistic Expectations

- Yes, some physical and electronic access control bypasses can take just seconds…
  But lockpicking isn't always "Hollywood" fast.

Focus on:

- **Quick bypasses** on common locks ***(what do you guys pick most?)***
- **Door configuration flaws**
  (ie. security plunger, gaps around the door)
- **Misconfigured PIR/REX** tied to **mag locks** or **electronic strikes**

Don't just know the "how" — **understand the why**

Bypass. Document. Recommend remediation.

Alarm systems

Alarm Systems Matter

- Is it in scope?
- Must be considered, especially for after-hours testing
- Just popping a door open can trigger a "Door Forced Open" alarm state



Alarm System Inception!!!

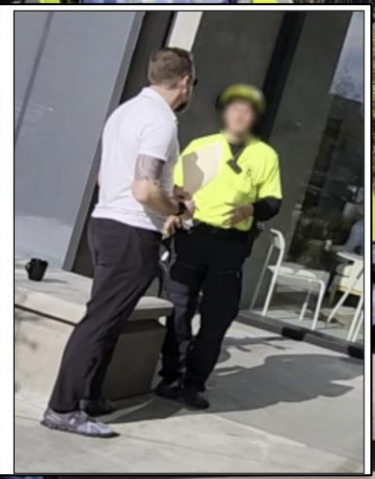
- Tamper alarms on access control panels and badge readers
- Understand how to bypass door contact sensors *(reed switch, magnetic contacts, etc)*
- ***PRACTICE!***

Social Engineering: Myths vs Reality

Social Engineering is not Magic: You're not going to Jedi-mind-trick everyone

It is not as easy as many people believe it is, but it can come natural to others…





- *Improvisational Skills are very important.*
- *Understand regions, basic psychology, dynamics.*
- *You can plan for months, memorize a script, and setup tools…but if that script changes, and you are unable to think on the fly, you will get caught.*

Disguises: Myths vs Reality

Hollywood often shows impersonating an officer, first responder, lawyer, etc.

In the United States and many other jurisdictions, it is illegal to pose as:

- **Law enforcement *officers***
  (local, state, or federal)
- **Firefighters or emergency medical personnel**
- **Military personnel**
- **Postal workers and mail carriers**
- **Utility workers from regulated public utilities**
  (in some states)



DISGUISES: MYTHS VS REALITY

- Doesn't have to be like Mission Impossible!
- *Quick, easy, and you must know the basics.*
- *Superficial changes such as altering your shape, body language, and clothing color*
- *Makeup isn't always needed, but ALWAYS requires skill and a specific purpose.*
- ***PRACTICE! Blend in and disappear!***







HOLLYWOOD: MYTHS VS REALITY

High-Tech Toys Rarely *SAVE* a Bad Plan:

Fancy toys and custom tools can enhance capabilities, but they won't fix poor recon, bad timing, or ignoring human factors. Even if you have a fancy 0-day!

Understand the target.

Have a plan that includes:

- A solid guise and believable story
- A look, walk, energy that makes you forgettable
- A working knowledge of the tools and attacks that you'll utilize based off of your reconnaissance.

HOLLYWOOD: MYTHS VS REALITY

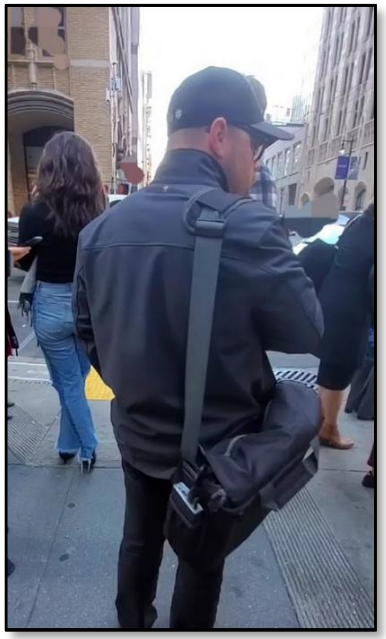


Mr. Robot badge cloning gets it right!

HOLLYWOOD: MYTHS VS REALITY

Badge cloning in real life: Concealment and movement are key!



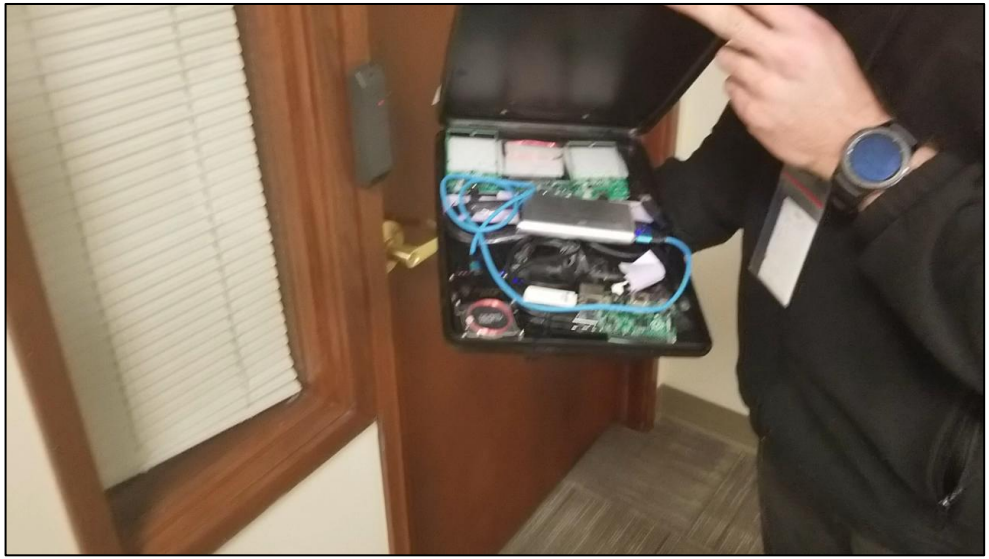




HOLLYWOOD: MYTHS VS REALITY

Badge cloning in real life:

- Concealment and movement are key!
- Replaying credentials with our old badge cloning clipboard - (The original *“Covert Clipboard”*)

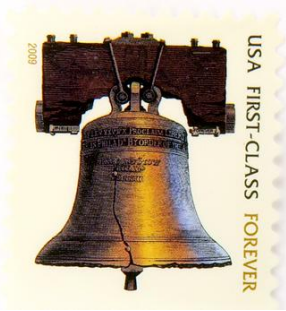




HOLLYWOOD: MYTHS VS REALITY

Badge Replay via Implants and Fake Readers (a little SE)

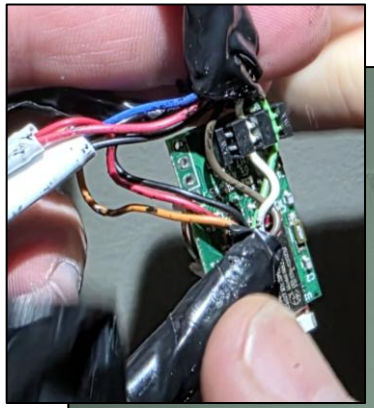
- Implants can help intercept and replay badge reads + PINs in real time. ***Destructive?***
- Readers like Doppleganger







- ESPKey Wiegand (Wi-Fi) *BETTER imo*
- BLEKey (Bluetooth Low Energy BLE)



REAL-WORLD MISTAKES TO AVOID

Let's discuss...



Destructive Entry

- Snapping shackles, cutting fences, damaging cameras = Automatic Fail.
- Even *accidental* destruction must be avoided.





Test in Production? Noooooooo

- Just because you watched a few Youtube videos from LPL or picked up some tools at a Lockpick Village does not mean you are ready to start raking locks and dragging magnets across things.



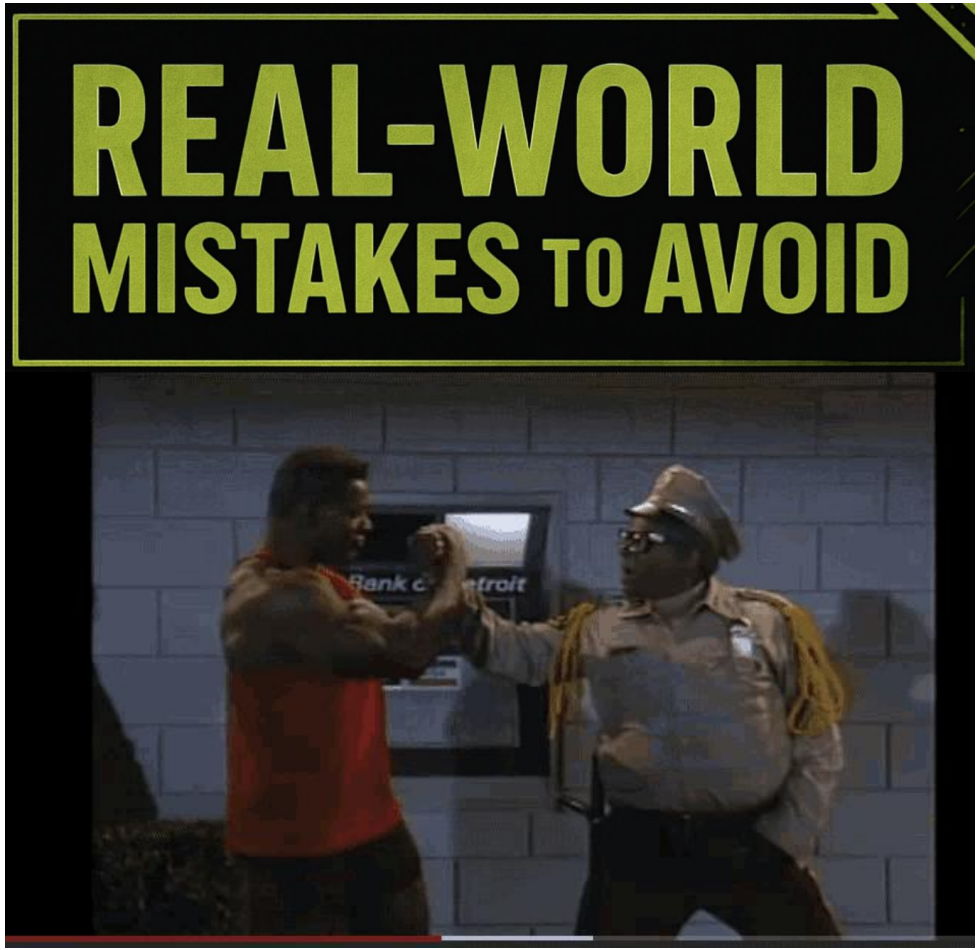
- **Caught by Security?** If they are aggressive and you do not believe they could fall victim to social-engineering *(fake LoA, etc),* de-escalate immediately. Calmly tell them what you have and pull out the “Get Out of Jail Free” letter if necessary.

- ***DO NOT RUN!*** *You’re a professional. Don’t become the criminal. If approached by law enforcement or anyone else, stay calm - you're authorized to be there.*

- **Wrong Building? Wrong Floor?** Be honest. If you broke into the wrong suite, plugged in and scanned the wrong network, you would be honest, wouldn’t you?

- **Prior Damage Detected? Stop and report** it *immediately* to your client POC (Point of Contact).





Aggressive Confrontations:

- **ALWAYS de-escalate!** Verbal or physical aggression gets you fired *(or arrested).*
- This type of confrontation isn't the same that we teach for social engineering with being firm or pushy with your requests.

Physical Altercations:

- Hands off employees. Hands off guards. *It should never get to this!*
- Do EVERYTHING within your power to comply, de-escalate, or walk away.
- Even if they initiate it, only protect yourself. If possible, do not retaliate.



Bribery or Coercion:

- Social engineering must remain ethical and within engagement rules.
- **EXAMPLE:** Never offer money or gifts to manipulate a target. This is a big **no-no**, especially in the federal arena.



Out-of-Scope Activities:

- Covert Entry assessments are dynamic so you will need to keep things broad. If it's not within the Rules of Engagement (RoE), *don't do it*.

- **Respect the Scope**: Memorize your Rules of Engagement (RoE).

SAFE, LEGAL, AND ETHICAL PRACTICES

Understand The Laws!

Have a basic understanding of what's legal and what isn't in this line of work for S&L and Federal.

- Surveillance Laws:
  - Audio / Video Recording, Wiretapping, GPS tracking, etc.
- Rights to Privacy
  - *"Assumed Privacy"* vs Peeping Tom
- Eliciting information
- Trespassing

Types of Entrants

- **Invitee:** Mutual benefit, usually commercial (e.g. customer in a store)
- **Licensee:** With permission, but for their own purposes (e.g. law enforcement, utility worker)
- **Trespasser:** Without permission or legal right.

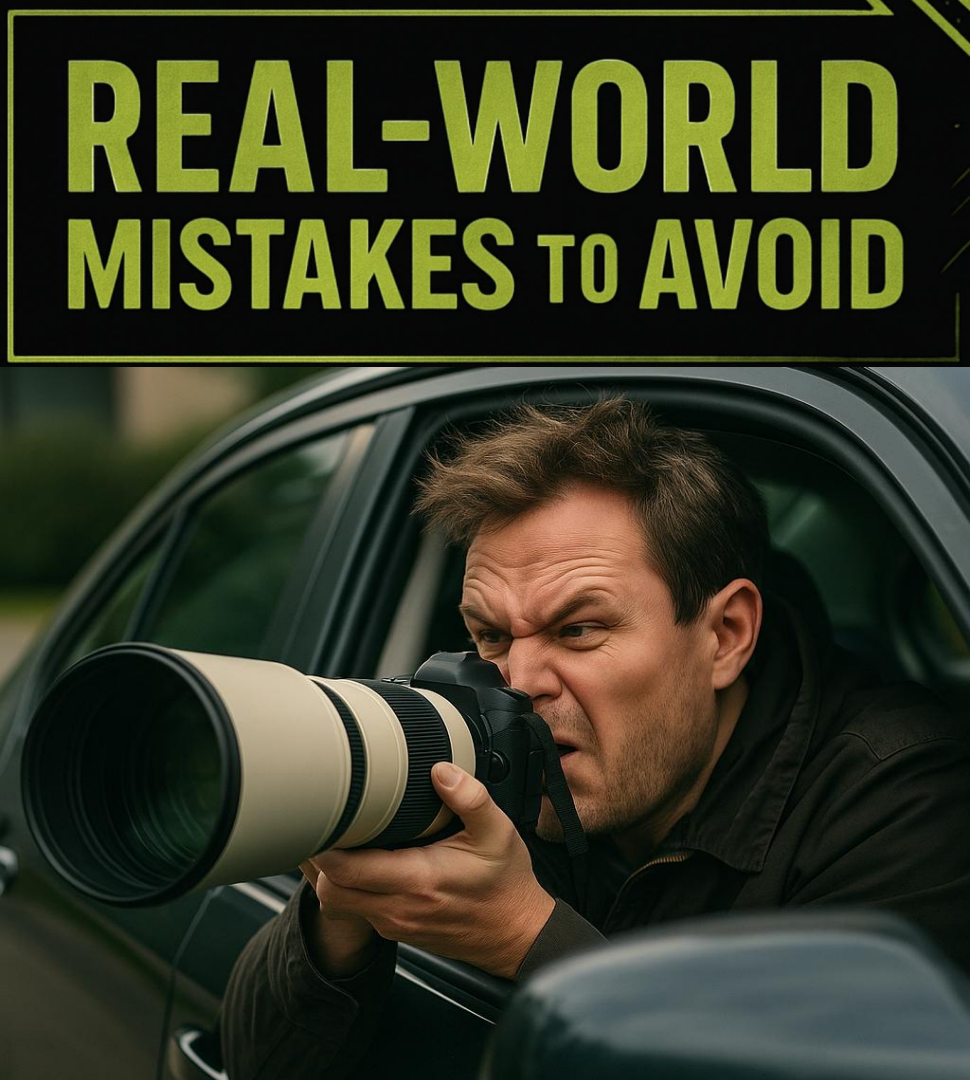
REAL-WORLD MISTAKES TO AVOID

Parkour Gone Wrong:

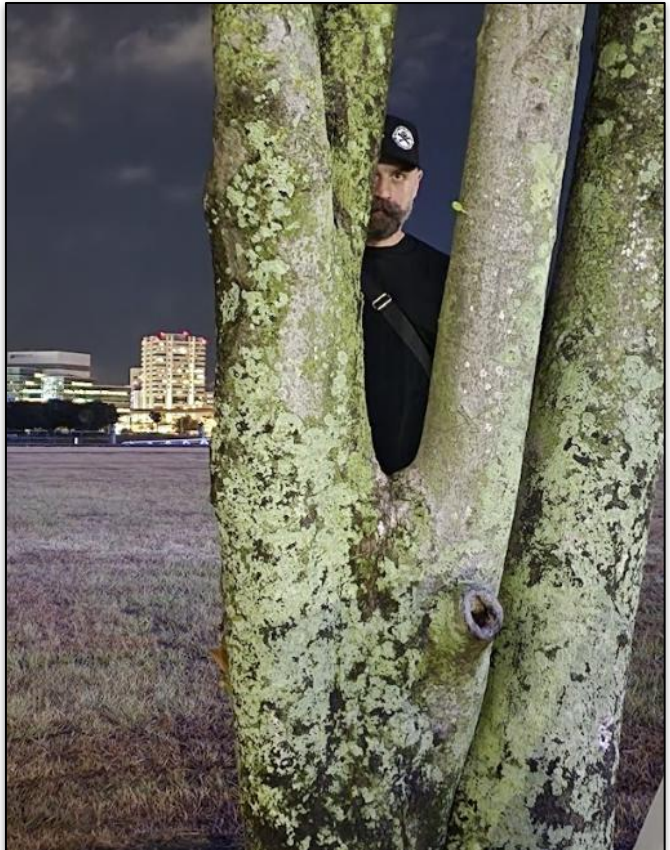
- No reckless climbing, scaling, or jumping over dangerous obstacles.
- Risking injury (or death) is never worth it for an assessment.

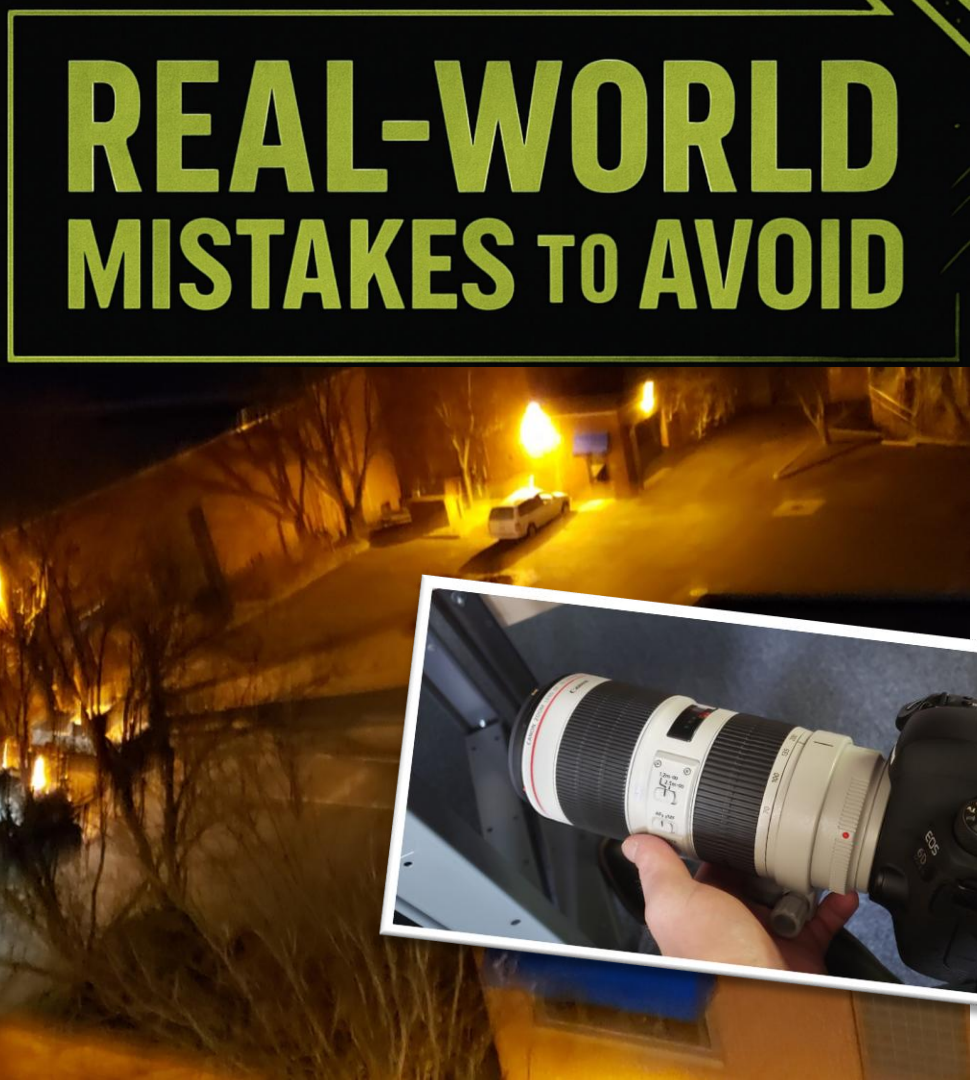






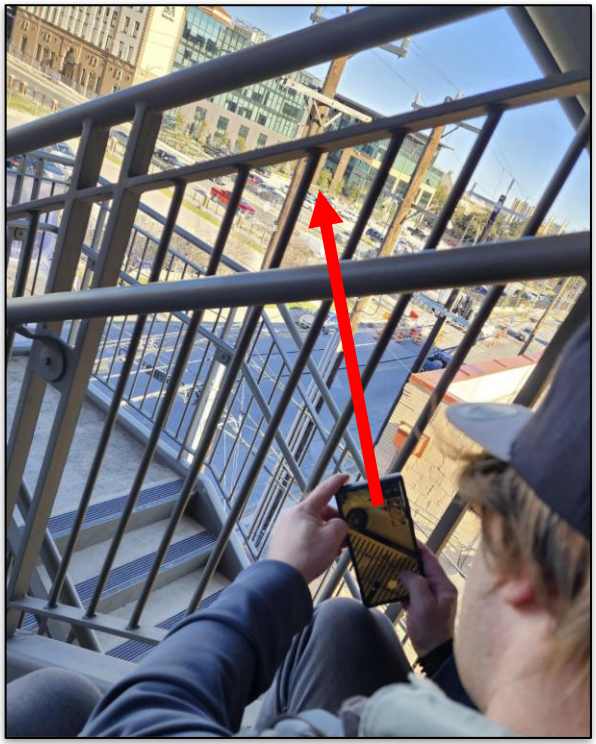
Surveillance Screwups

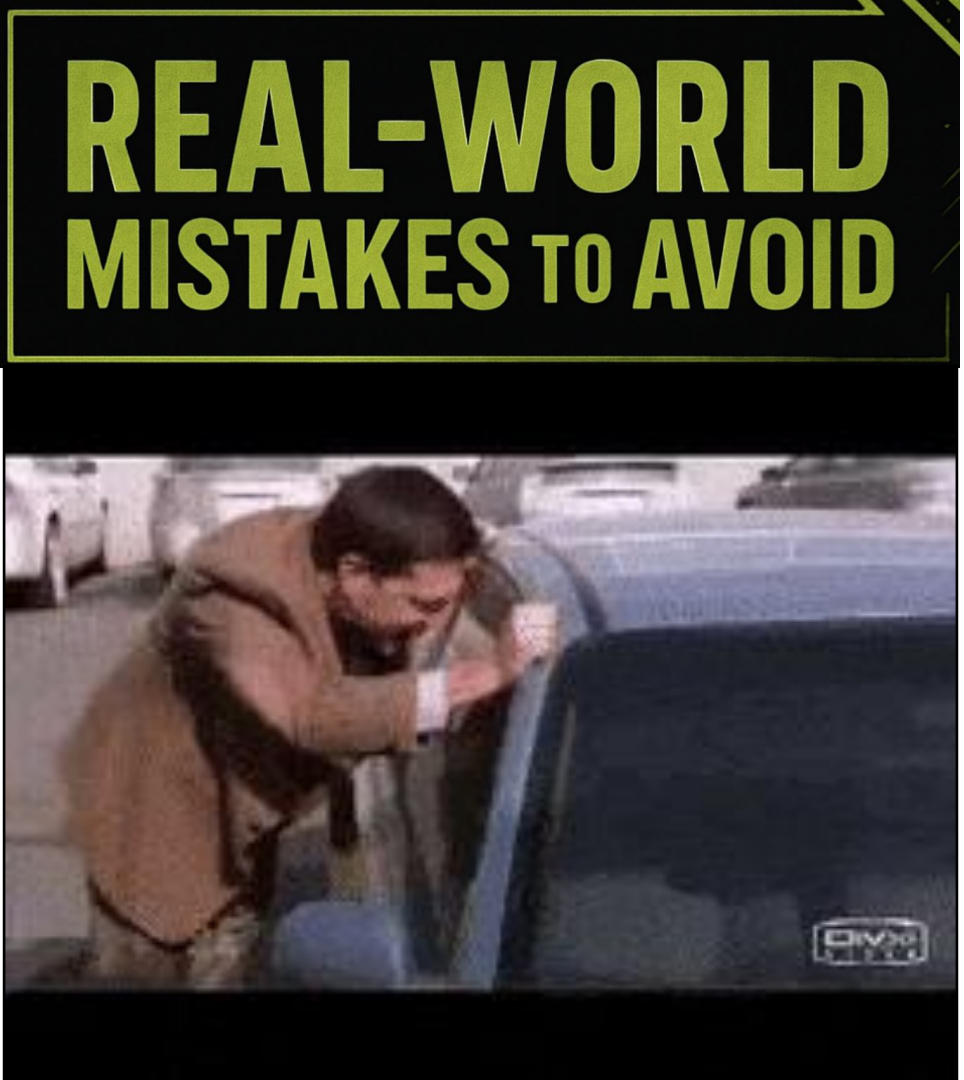




Surveillance Screwups

- A better way

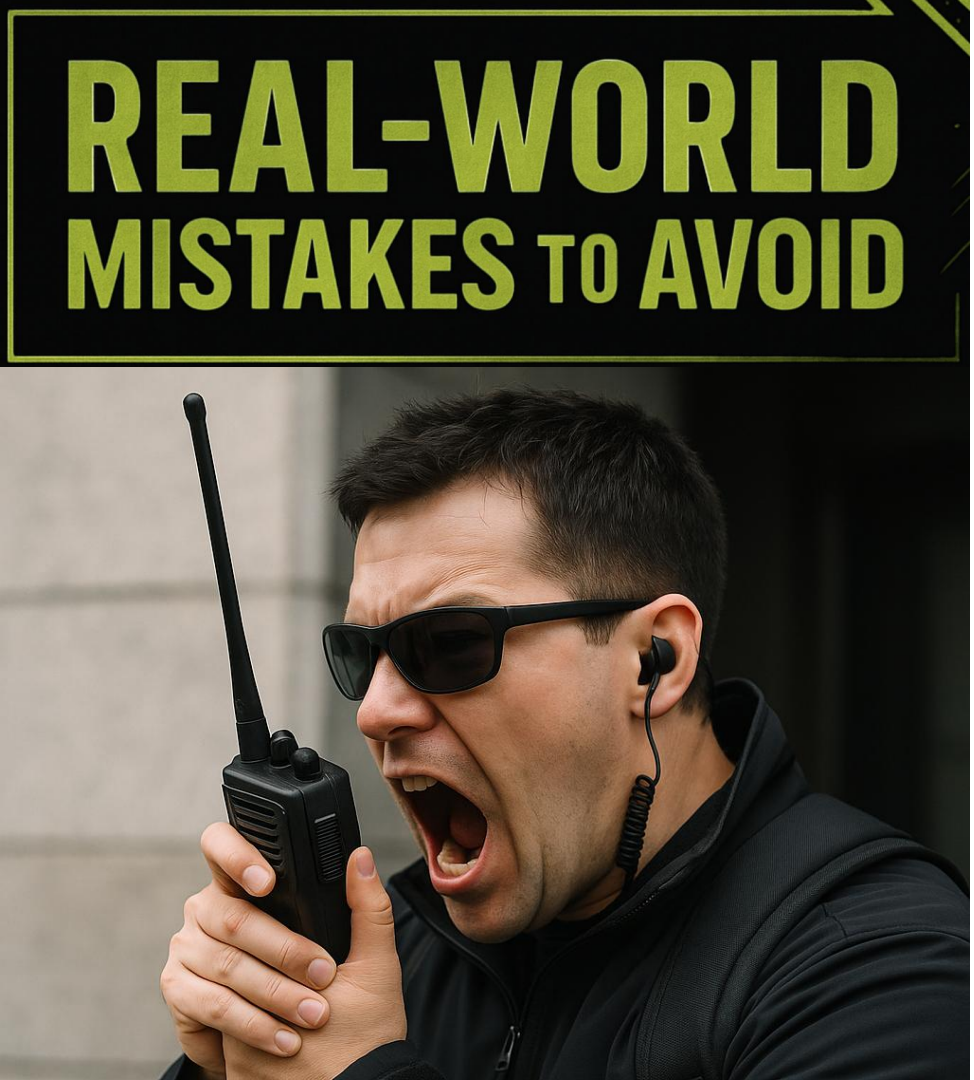




Surveillance Screwups

Got a vehicle?

- Turning off the headlights and interior exit lights
- Consider two vehicles.
- *Quit driving in circles!*
- DON'T accidentally set off the alarm!



Surveillance Screwups

Got a team? *(Red, Tiger, Pink Elephant)*
Communication is key!

- Know how to use the radio, encrypted comms, etc.
- Make sure your team understands the call signs and key words.
- Avoid useless chatter.
- Avoid "Radio Check" on-site! Test comms before you go!
- FCC laws are important.
- **Have a backup in case radios fail.**

TOOLS THAT WORK: (AND BEST PRACTICIES)

Hollywood's Junk

1. Lock picking
2. Social engineering
3. Destructive entry
4. Overly-complicated technical attacks
5. Unrealistic disguises

WeHackPeople's Covert Entry TOP 10

1. **Security Awareness**
   (Tailgating, SE, OSINT, Propped open, etc)
2. **Misconfigured Doors and Hardware**
   (Latch Slipping, O-UtD, Crashbar, J-Tool, etc)
3. **Misconfigured REX Sensors**
   (Canned Air, Handwarmers, etc)
4. **Unencrypted Badges**
   (Badge Cloning)
5. **No PIDs / Tamper Alarms Inactive**
   (Electronic Access Control implants)
6. **Port Hardening**
   (Rogue peripherals, DHCP active, etc)
7. **Default Physical Keys / PINs**
   (Keyed-alike panels, pins, etc)
8. **Weak Physical Locks**
   (Jiggling, Lock picking, shimming, etc)
9. **Continued Monitoring**
   (No incident response, 24x7 monitoring, etc)
10. **Loading Bay / Service Elevators**
    (Often left open or no badge restriction, etc.)

TOOLS THAT WORK:
(AND BEST PRACTICIES)







COVERT CARRY:

Years of research, testing and practice to reduce a back pack's load of tools into a concealable solution.

TOOLS THAT WORK: (AND BEST PRACTICIES)



Covert Entry Wallet

https://wehackpeople.wordpress.com/2019/10/10/lock-pick-concealment-edc-wallet/

- Scapular lock pick set from SEREPICK
- Flat tension tool (*this is from a separate pick set*)
- Quick Stick
- EZ Decoder
- Plastic shim that is cut to fit and folded in half
- Custom We Hack People RFID testing card
- Blank CAC card
- Gaffer tape (wrapped around part of my custom-cut plastic shim

War Stories & Lessons: Examples



- Security guards and control rooms
- Client's burning the operation before it even begins

Simply cannot be charmed and wants none of your ish…

QUESTIONS / CLOSING

Professional Mindset for Covert Entry

- **Be Forgettable, Not Famous**:
  You should *never* be the story after an engagement.
- **Protect the Client's Trust**:
  Always remember: you represent *them*, not just yourself.
- **Stay Professional, Stay Safe**:
  Reputation takes years to build, seconds to lose.
- **You're there to help!**



“I got robbed by a sweet old lady on a motorized cart.
I didn’t even see it coming!”

STAY IN TOUCH



WeHackPeople.com
Blog and Presentations on Covert Entry,
Red Teaming, and Social Engineering
/wehackpeople *covertentry*



DARK WOLF SOLUTIONS

DarkWolfSolutions.com
Penetration testing and security solutions for
commercial, DOD, and Intel community.

Tim Roberts

Tim.Roberts@DarkWolfSolutions.com
@covertentry

Brent White

Brent.White@DarkWolfSolutions.com
@BrentWDesign