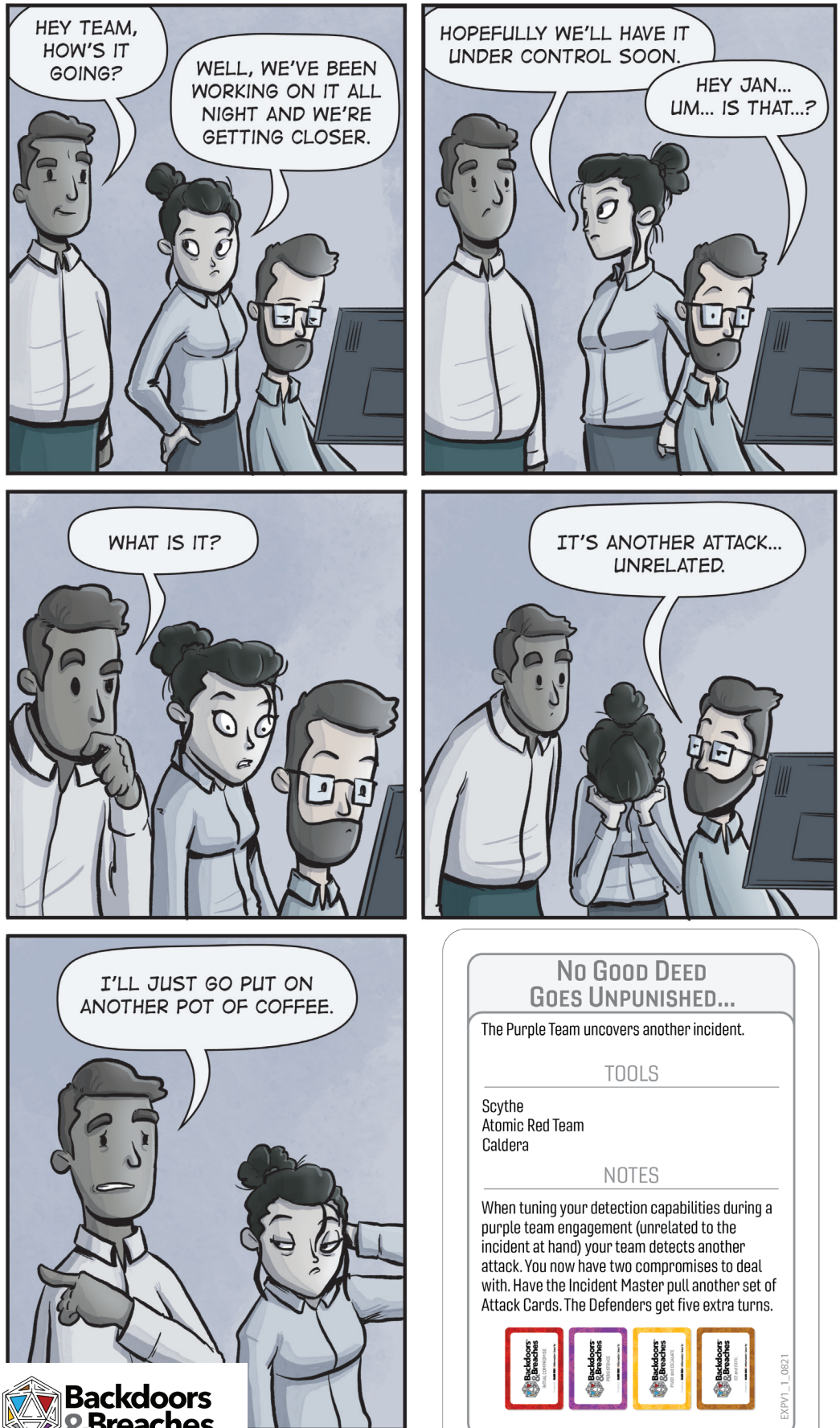
GIFDGK#

_ _ _ _ _ _ _#

S V K K V I K F X V K Y V I

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _



No Good Deed Goes Unpunished...

The Purple Team uncovers another incident.

TOOLS

Scythe
Atomic Red Team
Caldera

NOTES

When tuning your detection capabilities during a purple team engagement (unrelated to the incident at hand) your team detects another attack. You now have two compromises to deal with. Have the Incident Master pull another set of Attack Cards. The Defenders get five extra turns.

EXPV1_1_0821

Backdoors & Breaches

PROMPT#

INTRO

We have a few sayings at Black Hills Information Security that help remind us of who we are and why we do what we do. "Better Together" is one of those and is infused into all that we do at BHIS. We can't do life alone... and why would we want to?

I am grateful to be the editor-in-chief of PROMPT# because that means I get to bring together infosec subject matter experts, creative artisans, and a dedicated production and logistics team.

The zine you are holding in your hands is three months of work contributed by many, all banding together to educate, entertain, and create something that's never been done before. When John asked us to create a zine, we had no idea how to do that — but we worked together to figure it out.

We hope you enjoy the articles, interviews, mixtapes, challenges, feedback from the community, coloring contest, and the comic book based on a real-life penetration test.

- Jason Blanchard, aka @BanjoCrashland

CREDITS

Publisher
John Strand
@strandjs

Editor-in-Chief
Jason Blanchard
@BanjoCrashland

Designer & Illustrator
Caitlin Cash
caitlincash.com

Editor
Kassie Kimball
linkedin.com/in/kassiekimball

Associate Editor
Deb Wigley
@debthedeb

Preuph-Reidur
Madeleine Songer
linkedin.com/in/madeleine-songer

CTF Engineer
MetaCTF
metactf.com

Cover Artist
Scott Saslow
scottsaslow.com

Coloring Contest Artist
Alessandro Micelli
@themicellis

Other Contributors
The Traveler, Bradley Samuelson, Angelica Guevara, the team at BHIS, and members of our awesome community!

COMIC BOOK

Writer
Jamie Frevele
@jamiefrevele

Artist
Joe Eisma
@Supajoe

Colorist
Shari Chankhamma
sharii.com

Letterer
Taylor Esposito
@TaylorEspo

Original Story
Ralph May
@ralphte1

BLACK HILLS Information Security
115 West Hudson St.
Spearfish, SD 57783
Contact Us: 701-484-BHIS / info@promptzine.com
PRINTED IN CANADA. POLYBAGGED IN CANADA. CARDS & STICKERS PRINTED IN USA.

SECURITY & DEVELOPERS: BETTER TOGETHER

BY BRIAN "BB" KING

Years ago on a webapp test, I found a place where the app was returning raw error messages from the framework. The scanner I was using flagged it based on the word "EXCEPTION" in the response.

I was on the corporate security team, so rather than digging into how an attacker might exploit this, I just reported it as-found; a screenshot of the HTTP response with "EXCEPTION" highlighted, some words about how "verbose error messages" are bad, and I moved along to the next thing.

Jump to the retest. The dev team says everything is fixed. Sure enough, the scanner doesn't report the issue this time.

Now, I need to see if the fix was complete and whether it may have introduced new problems. But when I manually send the same request that triggered the error in the original test, the response still has a full stack trace. The verbose error message is still there. Why didn't it get flagged?

I scroll up, and where the original test showed "EXCEPTION," this one had

"E-X-C-E-P-T-I-O-N"

The developer's "fix" was to make sure the scanner wouldn't find the word that was highlighted in the original report.

Seriously?

Are we not speaking the same language here?
In what way is this better?

As I would find out, I wasn't far off. **Security teams and development teams do speak different languages.** The trouble is that few of us are aware of that. We assume that because we're all into low-level computery things, we must share a common outlook and vocabulary.

This is the worst kind of misunderstanding: the kind where you're confident that there is no misunderstanding. It would have been better to see blank stares from the developers when I gave them the report than to have this.

As I thought about how to respond to this, um, ***creative solution***, I remembered one of the developers from previous meetings — Victor. He seemed to be paying more attention than most. He asked good questions about the issues. He once even restated one of the security team's recommendations in different words that seemed to resolve the uncertainty in the dev team. After that, the bug we'd been talking about was fixed in the next build.

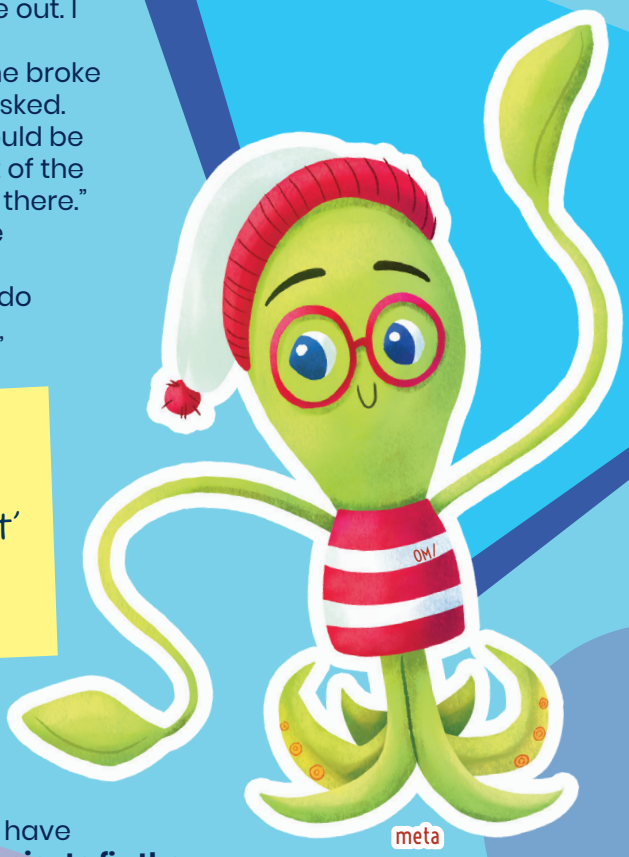
I thought maybe Victor could help me out. I went to his desk and said hello.

"Did you see this thing where someone broke up the word 'exception' in responses?" I asked. "The only reason I can think to do that would be to throw off automated analysis. The rest of the response is the same. The problem is still there."

Victor laughed and looked across the cubicle farm. "I think I know who did that."

"Don't tell me. But why would anyone do that? It's obviously not fixing the problem, right?"

"Well, honestly, sometimes it's hard to tell exactly what these 'security defect' reports are asking us to change," he explained.



"Some of these attacks are complicated, or they use some crazy tool you got off GitHub. You know we're blocked from 'hacking tools,' right? All we have to go on is the pentest report. **It can be easier to fix the obvious thing so we can get back to doing real work.** At least then we can close the defect ticket and get it off our list."

Real work. Right. **A person becomes a dev because they like building things.** Maybe they like optimizing existing features too, but that's still a creative pursuit. Building new things and fixing defects that get in someone's way is satisfying in a way that closing an attack vector that's not being actively exploited will never be.

"Look, Victor. You find this security stuff interesting, right? I've seen you in meetings."

"Yes, I do! I'm actually working on an appsec-focused certification to help round myself out a bit. I like to know what the security team is talking about, and some of the exploits you find are actually pretty cool."

"Let's try something. I'll help you with your security studies, and maybe you can help me communicate better with the dev team. They respect you, and they know you understand that world because you live in it."

He agreed.

After that day, **Victor and I had an ongoing exchange of information,** questions, link sharing, and advice. We'd meet for lunch occasionally, but it was mostly chats and emails.

That open door did wonders for the relationship between the dev team and the security team. I would ask Victor for feedback on how we were reporting things; how would this come across to the dev team? He would help me gain perspective on what the dev team had to balance against the issues I was reporting. I had no idea of the hoops they had to jump through to fix things that seemed simple to me. The side effects. The lack of time and resources. The regression testing. He'd help me rephrase things so the message was clearer to the devs. Through these conversations, he knew what was coming in future reports, and was ready to help explain things to his peers when there were questions.

The security team had an advocate on the development team. Pentest reports were no longer, "security has some random new complaint," but "security sees a problem here — do we understand the cause? What's the best solution?" Not every time, of course. But sometimes. And ever more often as time went on. When they got into devops, they came to us to help build paved roads — those pre-approved components — for things they'd use over and over. We solved problems up front.

I got to help Victor study for his infosec certification and introduce him to pentesting. Teaching is a great way to find your own gaps in understanding, so we both got better at security together. He earned his cert right on schedule and I bought him lunch to celebrate.

(On top of it all, I had a friend who could tell me which of the JavaScript Frameworks-of-the-Week were worth paying attention to, and which I could safely ignore for a while longer.)

Security team. Development team.

Always better together.

WARHORSE

ATTACK AUTOMATION FRAMEWORK

CREATED BY RALPH MAY

>WHAT DOES WARHORSE DO?

Warhorse is an attack automation framework that helps deploy infrastructure faster for security assessments.

>WHY DID YOU BUILD IT?

Warhorse has three primary goals: speed up infrastructure deployment times, integrate TTP's, and use better OPSEC through code.

>HOW DO I USE IT?

Simply put – clone the git repo, modify the configuration YAML file, and then run Ansible deploy.
Full documentation can be found at: https://docs.war-horse.io/

>WHERE DO I GET IT?

https://github.com/warhorse/warhorse

Read about Ralph's real-life pentesting adventure starting on pg. 23!

InfoSec Creator Mixtapes

Hacking Your Health is a community dedicated to helping others understand how to hack their mind, body, and business.

Ben Canning
David Kennedy
Hacking Your Health

https://wehack.health

The OSINT Curious Project is an OSINT-learning catalyst, providing quality and actionable open-source intelligence news, original blogs, instructional videos, and livestreams.

#OSINTCURIOUS
OSINTCURIO.US

The OSINT Curious Project

OVBZRGEVP
R13

John Hammond is a cyber security researcher and educator who showcases free programming tutorials, CTF video walkthroughs, malware analysis, and other cyber security content online.

https://youtube.com/johnhammond010

Making Community Better

BETTER TOGETHER

R6 MAGXJ

MIXTAPES ARE A TOKEN OF LOVE AND ARE ENJOYED BY FRIENDS


Ippsec's channel is one of the most recommended places for people to get started in Penetration testing. He walks through HackTheBox machines every week while explaining the thought process.
IppSec
https://ippsec.rocks
DARKNET DIARIES IS A PODCAST ABOUT HACKERS, BREACHES, SHADOW GOVERNMENT ACTIVITY, HACKTIVISM, CYBERCRIME, AND ALL THE THINGS THAT DWELL ON THE HIDDEN PARTS OF THE NETWORK.
DARKNET DIARIES
HTTPS://DARKNETDIARIES.COM
JACK RHYSIDER
DARKNET DIARIES
Simply Cyber is an information security YouTube channel designed to help individuals go further, faster in the information security field, through weekly videos and livestreams.
Gerald Auger
https://www.simplycyber.io
SIMPLY CYBER

BETTER TOGETHER WITH

CANARY ACCOUNTS IN ACTIVE DIRECTORY

by John Strand

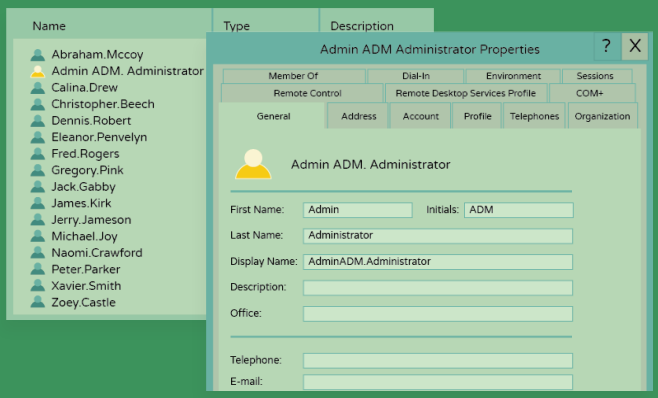
Cyber Deception gets a bad rap.

Many in the industry feel that it is something that should be done after everything else is done. Like an afterthought. There is also a belief that it takes a lot of time and money to get it right.

None of that is true.

Let's talk about how we can implement deception quickly and easily in your environment in under an hour (and as a bonus, it will catch almost every post-exploitation, red team, or hacker group.)

First up, we need to create a fake user, or as we call it, a "canary user." Below, you can see that I created a user account that is called Admin Administrator. I know that some will say that this account is a bit too "on the nose," but it does not matter... at all. When attackers try and elevate privileges in an environment, they are not looking for accounts to break into. Rather, they are going to spray all the active accounts with a common password, like "$pring2022!"

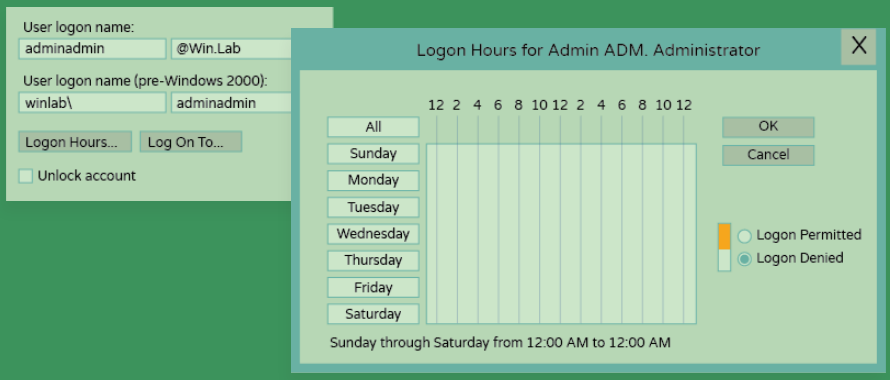


Next, we will need to set a password and log in to the account. This is necessary, as an account that has never been logged in to will have a last logon time of January 1, 1601 (which is epoch time for Active Directory accounts). Most password spraying tools will skip accounts that are locked out or have never been logged in to.

As a side note, set the password as something exceptionally long and complex. It does not matter from the attacker's perspective. They will automatically try to log on using a script or a tool. We just want to make sure that your honey account is not a direct route to accessing other systems.

In addition to setting the long password for the honey account, we want to disable the account without "disabling the account." We can do this by disabling the logon hours for the account.

You can see this below:



Next, you will need to create a rule in your SIEM (Security Information and Event Management). The rule should be simple. If anyone tries to log on to the honey account, an immediate critical alert should be fired. In other words, this rule will effectively have 0 false positives.

Keep in mind, it is not important if the attacker successfully logs on. It is just that someone tried.

To test it, we recommend that you use a tool like DomainPasswordSpray from @dafthack:

```
PS C:\tools> Invoke-DomainPasswordSpray -Password $pring2022!
[*] Using C:\temp\UserList.txt as userlist to spray with
[*] Password spraying has started. Current time is 10:19 AM
[*] This might take a while depending on the total number of users
[*] SUCCESS! User:Christopher Password: $pring2022!
[*] SUCCESS! User:Dennis Password: $pring2022!
[*] SUCCESS! User:Gregory Password: $pring2022!
[*] SUCCESS! User:Jack Password: $pring2022!
[*] SUCCESS! User:Jerry Password: $pring2022!
[*] SUCCESS! User:Michael Password: $pring2022!
[*] Password spraying is complete
[*] Any passwords that were successfully sprayed have been output to
C:\temp\sprayed-creds.txt
PS C:\tools>
```

You can get it here:
https://github.com/dafthack/DomainPasswordSpray

Remember, the goal is not for DomainPasswordSpray to successfully log on to the account. It is just that it tries. An alert should be fired. Every SIEM has a different way of creating rules. Work with your team to set this one up. It should not be that hard.

The goal of this is to set effective traps in the pathways that attackers are going to use. If you were to have a honeypot system, the odds of the attacker finding it and attacking it are pretty low.

But an account in Active Directory?
They are going to password spray.
They are going to hit your imaginary account.
You are going to detect them.

As my dad said, an imaginary friend is still a friend.

ADHD

ACTIVE DEFENSE HARBINGER DISTRIBUTION

What does ADHD do?

Active Defense Harbinger Distribution (ADHD) is a collection of open-source tools, provided as a distribution built on top of Ubuntu 20.04.

Why was ADHD created?

ADHD was created to facilitate the principle of active defense, providing tools that help actively defend your environment from malicious attackers. Tools are categorized under Annoyance, Attribution, and Attack. These have been collected with the overall goal of making an attacker's life more difficult and wasting as much of their time as possible.

How do I use it?

Download and load the virtual machine image, or give our beta buildkit a try. For documentation regarding each tool, refer to ADHD's official documentation here: *https://adhdproject.github.io/#!index.md*

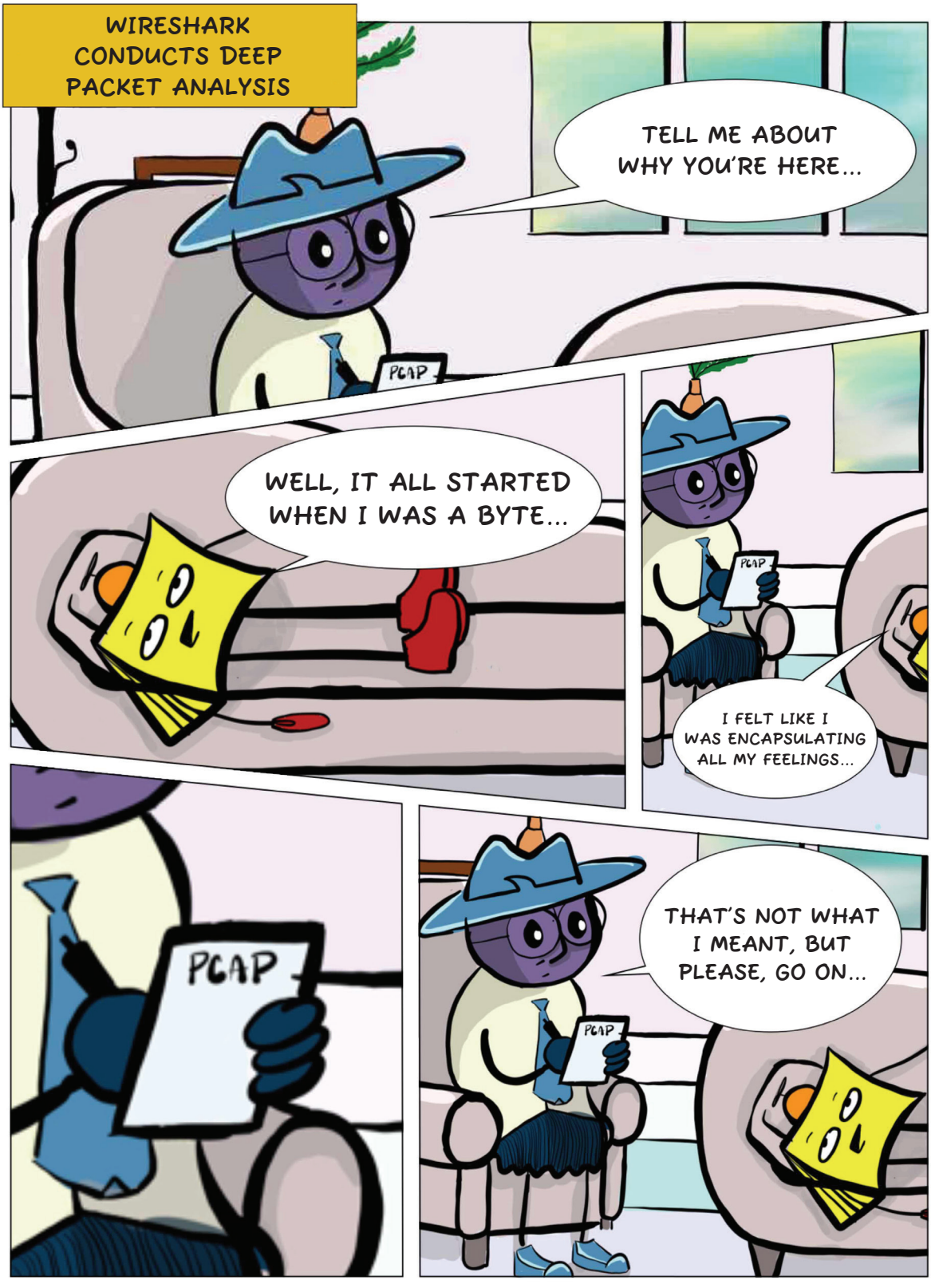
Where do I get it?

Download the buildkit, as well as any of the tools we've forked and updated, by visiting our GitHub project: *https://github.com/adhdproject*

Download the OVA here:
https://adhdhost.s3.amazonaws.com/ADHD4/ADHD4-sha1.ova

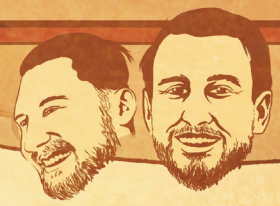
Filename: ADHD4-sha1.ova
MD5: 3b0cc1846f86acac875679aaabdc8552
SHA1: 19f9f8e2be0fceffaf6e177123f78d896e0850bd
SHA256: b461505166a930b5503f19a9a9e500abe62c924234dbc160f3fa5b2e7c204a5c

CREATED BY BHIS, MAINTAINED BY ACTIVE COUNTERMEASURES



BY ANGELICA GUEVARA

THE CROW'S NEST



R25:DLZHK

Many on our team recently shared with us their stories about how they came to join BHIS.

If you're on the job hunt, we hope these can provide some encouragement for you in your journey. You never know where you'll find your big break!

~Kassie, aka @sneaky__space

WANTED:
Plain text document version of resume,
will not open doc / docx files.
Applicant must have:
- Linux
- Windows
- Network

Meet in alley behind sushi restaurant on St Joseph.
Send resume to weirdjobpost@fakemail.com

My wife thought submitting a resume and responding to this post was the worst decision I had ever made and that she would never see me again. I replied to the ad and agreed to meet in between my appointments with customers. While I was wearing a tie, John Strand said the following:

- "You can connect to TCP port 70000 in Bash... but how???"
- "How Archer-esque of you. If you wear the tie to work here, you will be fired."

Eventually, John called and made a job offer I couldn't refuse.... And that was that.

-Jordan Drysdale

After I experienced downsizing at my previous job, my friend Jordan asked if I would help him out on a few projects at BHIS. He invited me to an interview with John (but warned me explicitly not to wear a tie). When I met John, he looked at me and said, "You're Kent, right? Cool. Welcome to the team; want lunch?" And that was it. What followed was six months of contracting work, trying to kick-butt and organize BHIS's infrastructure.

I remember, albeit somewhat foggily, my wife and I were in Deep Ellum in Dallas, Texas for lunch on Easter Sunday. I may have been a few libations in when John called.

"Hey listen, I know you've been working really hard for us and this is Easter weekend, but some things came up... Unfortunately, using you as a contractor going forward isn't going to work out."

My heart dropped. I loved the work I was doing, BHIS, the team, everything.

"So we're going to officially hire you. Can you start when you get back?"

And that was it — I became the newly employed Systems Administrator at BHIS.

-Kent Ickler

Having no formal training in information security, I was invited by my son to join the BHIS family.

Reluctant at first, he convinced me that I might be a good fit to share my embedded hardware low-level coding and RF radio experience. Being recently retired and not getting any younger, maybe his real motive was for me to challenge myself again (like the old days) and keep my brain active.

Regardless of the motivation, it was the perfect opportunity for me to bond with my son and get an appreciation for what he does; I won't pretend to understand the specifics (way beyond my paygrade). Suffice to say, I am grateful and humbled that John and the team have offered me this special gift. I'm proud to be part of this awesome family!!

-Ray Felch

So, BHIS is based in the Black Hills. I went to school at a place right in the middle of the Black Hills called Rapid City and there was a poster, just a one-page ad, for an internship, hanging on a bulletin board. It was my mom who actually noticed it and pointed it out. I think it said something like:

> "Do you like to break things? All you can drink Mountain Dew!"

I called the number on the flyer. John Strand answered and said nobody had called him in about six months; he didn't even think the flyer was there anymore. But here I am. He asked me a few questions on the phone and then decided to meet me. He lives about an hour away, so we set up a time and he took me to dinner — that was the first time I'd ever had sushi.

That was our interview. He hired me on as an intern while I was still going to college.

-Ethan Robish

A friend of mine who worked for John Strand told me there was a job opening. I sent my resume to John and he told my friend he thought that I was full of crap. He decided to meet me for lunch anyways and asked me to pick the spot. John wasn't a fan of the food, apparently, and he told his kids that they didn't have to eat it and could throw it away. Then he said he wanted me to do some 1099 work for him.

A few days later, he called and said he changed his mind: he wanted me to work full-time and wondered if I could be in San Francisco in a few weeks for my first on-site job. I had interacted with him for a total of about one hour at this point. I said, what the heck — YOLO — gave two weeks' notice at my other job and have been at BHIS for over seven years now.

-Brian Fehrman

Don't Go Alone

By Jason Blanchard

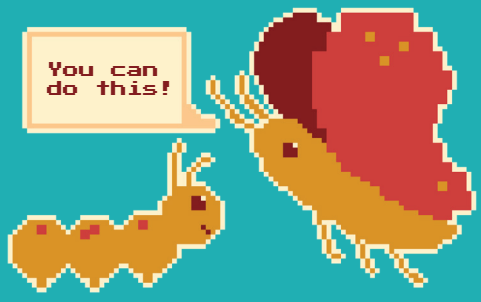
We all have informal mentors: teachers, supervisors, trusted colleagues, family members, etc. We might not view these relationships in terms of mentorship, but they do often fulfill that role. They help, advise, train, and support us through various aspects of our life.

But we're gonna talk about formal mentors. A formal mentor is someone you specifically reach out to and ask, "Will you mentor me?" This will be a person whom you hope to emulate in some area of your life, such as your career, hobby, or business.

Keep in mind: when you reach out to anyone, it doesn't mean they're going to say yes.

But that's not the important thing.

YOU are reaching out. YOU are taking the next step. ***To be mentored means you are taking responsibility for your own growth.***



Mentors help us figure out the "why" behind the "what." They guide us on the path to get to where we want to be. Needing a mentor doesn't preclude you from BEING a mentor. Everyone has room to grow, and everyone has skills, talents, and achievements they can use to help someone else.

How to Find a Mentor

- OSINT and recon skills
  > Use your skills to find the people who are doing the thing(s) you want to do.

- Personal connections and community networking
  > Reach out to that accomplished person in your life whom you admire.
  > Go to events, connect with people, check out the leaderboards.

- Organizational programs
  > Ask your organization if they have a mentorship program.

Qualities of a Good Mentorship

- Mentors don't come up with goals for you, but they can help you figure out what yours are (and then provide accountability).

- Mentors don't tell you what you "should" do... they make suggestions, not hard rules!

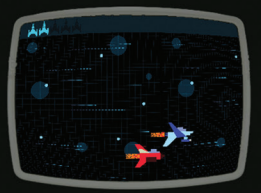
- Mentors listen more than they talk.

- Mentors don't use you to fulfill their own dreams or vicariously live out missed opportunities.

Find a mentor. Be a mentor.
We're all better together.

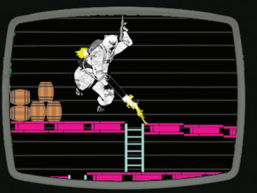

"Wild West Hackin' Fest is hands down my favorite conference and one I ensure I support and go to every year. It's such an intimate setting with friends, peers, and a welcoming community with some amazing talks and events. I'm a fan of WWHF for life."
– Dave Kennedy
WILD WEST HACKIN' FEST
JOIN US IN THE WILD WEST
DEADWOOD, SD
FEATURING:
HACKING LABS
NEW FRIENDS
OLD FRIENDS
BELLY LAUGHS
STEAK DINNER
SCENIC VIEWS
HISTORIC TOWN
MERRIMENT
trust us
AFFORDABLE TRAINING COURSES
INFOSEC CONFERENCE
COME ONE
COME ALL
ANNUAL EVENT
SPEAKERS!
SWAG BAG!
CHALLENGES!
ESCAPE ROOM!
IN-PERSON
HYBRID
VIRTUAL
WWW.WILDWESTHACKINFEST.COM

Collect Them All



ADVANCED NETWORK THREAT HUNTING
CHRIS BRENTON

ACTIVE DEFENSE & CYBER DECEPTION
JOHN STRAND

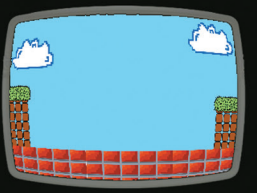


ADVANCED ENDPOINT INVESTIGATIONS
ALISSA TORRES

ATTACK EMULATION TOOLS
CARRIE ROBERTS

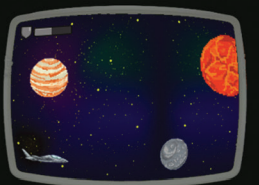
DEFENDING THE ENTERPRISE
JORDAN DRYSDALE

APPLIED PURPLE TEAMING
KENT ICKLER



SOC CORE SKILLS
JOHN STRAND

BREACHING THE CLOUD
BEAU BULLOCK



MODERN WEBAPP PENTESTING
BB KING

SECURITY LEADERSHIP
CHRIS BRENTON

RED TEAM: GETTING ACCESS
MICHAEL ALLEN

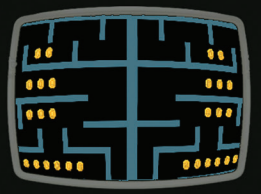
HACKEROPS
RALPH MAY

WINDOWS POST EXPLOITATION
KYLE AVERY

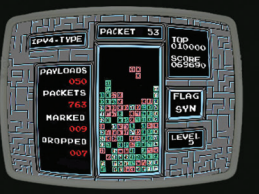
NETWORK FORENSICS: HUNTING WITH PACKETS
JONATHAN HAM

GETTING STARTED IN SECURITY WITH BHIS AND MITRE ATT&CK
JOHN STRAND

REGULAR EXPRESSIONS, YOUR NEW LIFESTYLE
JOFF THYER



ENTERPRISE ATTACK EMULATION AND C2 IMPLANT DEVELOPMENT
JOFF THYER



GETTING STARTED IN PACKET DECODING
CHRIS BRENTON

Caesar Word Salad

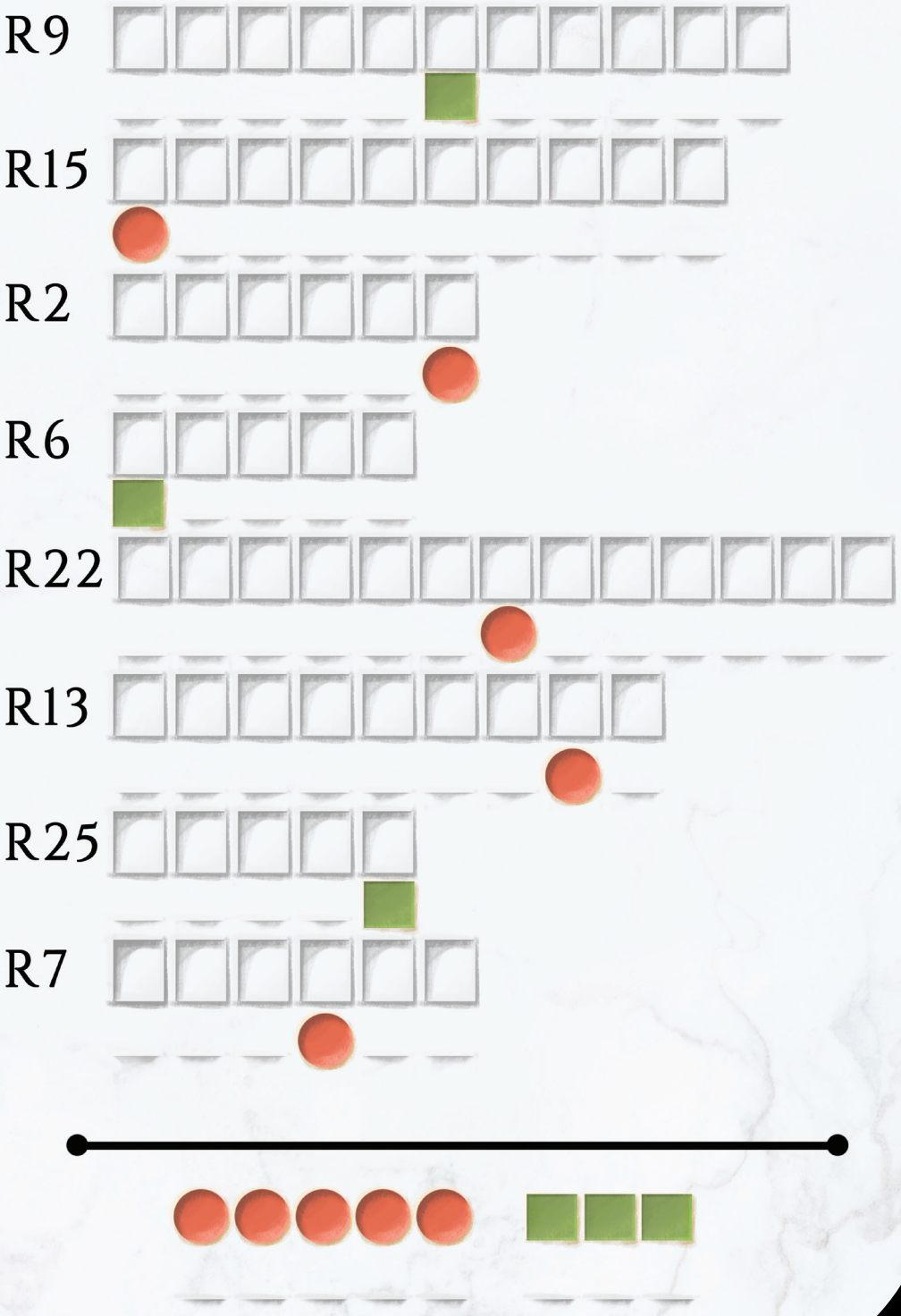
In cryptography, a Caesar cipher is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

(Source, Wikipedia)

Your mission, should you choose to accept it, is to find eight hidden encrypted words within this zine and decipher them, revealing the select letters to create two unique words (which were inspired by this issue's comic, "An Unlikely Alliance"). You'll then use those two words to gain access to five cyber security challenges, created by MetaCTF, when you go to: https://mctf.io/prompt2

After logging in or following the directions to create your MetaCTF account, you will see a section for "PROMPT#: Better Together" on your account dashboard. From there, click "Compete!" to access the challenges and hints. Additional instructions will be available inside.

(If you like, cut out the Caesar cipher decoder from the PROMPT# cover to help decipher the encrypted words.)


R9
R15
R2
R6
R22
R13
R25
R7

R7 LYH2LK

WINDOWS LOGS ARE A CRIME
YOU HAVE A POSSE

JOHN STRAND

One of the single biggest issues in security today is logs and logging.

We are logging a lot and detecting extraordinarily little. But we keep hearing about things like data lakes, data streams, data oceans, and data glaciers. *I may have made up a few of those*, but the core point with many of these technologies is to log more. Always log more.

And yet, our detects are still in the single digits from most SIEM (Security Information and Event Management) technologies. Worse, the vendors keep recommending logging policies that have us log more (always more) and they make more (always more) money on the amount we log.

It is a bad cycle, it is a crime, and it needs to stop.

Let's quickly go through a few folks and projects you should know about to get a better handle on Windows logging.

First, I want to introduce you to **Sysmon**. While most Windows endpoint logs are horrible (I am looking at you, System, Security, and Application), Sysmon is what you have been waiting for.

Sysmon logs what matters. With Sysmon, you get this:

```
Process Create:
RuleName: -
UtcTime: 2022-03-03 00:32:11.746
ProcessGuid: {b1a62ae4-0c8b-6220-930a-000000003100}
ProcessId: 4544
Image: C:\tools\TrustMe.exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: TrustMe.exe
CurrentDirectory: C:\tools\
User: DESKTOP-I1T2G01\adhd
LogonGuid: {b1a62ae4-45a9-621d-788f-080000000000}
LogonId: 0x88F78
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=512B9202BB2EACBFD0DA901C4FB59527,SHA256=B-
46DEA5319149E5AB16530DC3B2D3279192B98B90D5D1F96A7910
2B662BBE6CC,IMPHASH=481F47BBB2C9C21E108D65F52B04C448
ParentProcessGuid: {b1a62ae4-0c42-6220-
8f0a-000000003100}
ParentProcessId: 7448
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: cmd.exe
```

Here, we are capturing Event ID 1. It shows us the full path to the .exe, the process ID, the parent process ID, the hashes of the .exe, the original name of the .exe, and who created the .exe.

It is truly magic. And you need to log it. Today. Right now.

Some may say that you are already logging too much and Sysmon is an undue burden. Those straw men and women that I just created for this argument are wrong. *Do not give up logging something that is useful because you want to keep something with little to no value.*

To help you on the Sysmon Journey, I want to share some folks who are amazing.

OLAF HARTONG
@olafhartong

First up, Olaf Hartong (@olafhartong), who created sysmon-modular.

Sysmon-modular is a framework for creating Sysmon configurations that reduce the time and effort in creating a config for your environment. It will also reduce the overall noise from the Sysmon logs as well.

MICK DOUGLAS
@bettersafetynet

Next, I want to introduce you to Mick Douglas (@bettersafetynet).

Look, I have been teaching security for a while. Anytime I have a question on Windows logging (or life in general), the man with a banana is one of the first people I call. Seriously, he is awesome. He has lots of presentations and webcasts on defense. Here is one of his better ones — just Google: "Life is a Bit Easier with What2Log.com."

Next, let us look to Japan. Specifically, **JPCert**. This team has been doing an excellent job analyzing Windows and Active Directory (AD) logs, tuning in what logs and artifacts are generated, and which logs are key for understanding what is going on in an AD environment.

The first project they have that is awesome is LogonTracer. This is a tool that will help you understand what Windows logs can be used to better understand authentication.

They also have the Tool Analysis Result Sheet, where they analyzed many of the built-in tools that attackers use (i.e., psexec, powershell, etc.) and mapped what artifacts are created on a Windows system when they are run.

READINESS STATE	DESCRIPTION	READINESS CONDITION FEATURES
DEFCON 1	Breach imminent or occurred	Forensic imaging; Blocking techniques/tools (Server, Workstation, and Network)
DEFCON 2	Enhanced Measures	Event Forwarding (Workstation); Threat Hunting
DEFCON 3	Heightened Measures	Event Forwarding (Member Servers/apps); Network Device logging; Sysmon/EDR
DEFCON 4	Increased Security Measures	Audit policies; Event Forwarding (Domain Controllers); Network Monitoring; Centralized logs
DEFCON 5	Default Configurations	Vanilla OS/App/Device logging; No centralized logs

Finally, the BHIS SOC team has created an event logging resource that we share with our customers and the community at large. It even has a leveling system for what level of logging you may want to set up.

This project is what we use with our SOC customers as a starting point. It is maintained by Lord Monopixel IV of our SOC team.

As I said, logging in a Windows world is a crime. But you have a posse of great people to help deal with it. And in the process... Maybe, just maybe, you'll have fun?

RESOURCES:

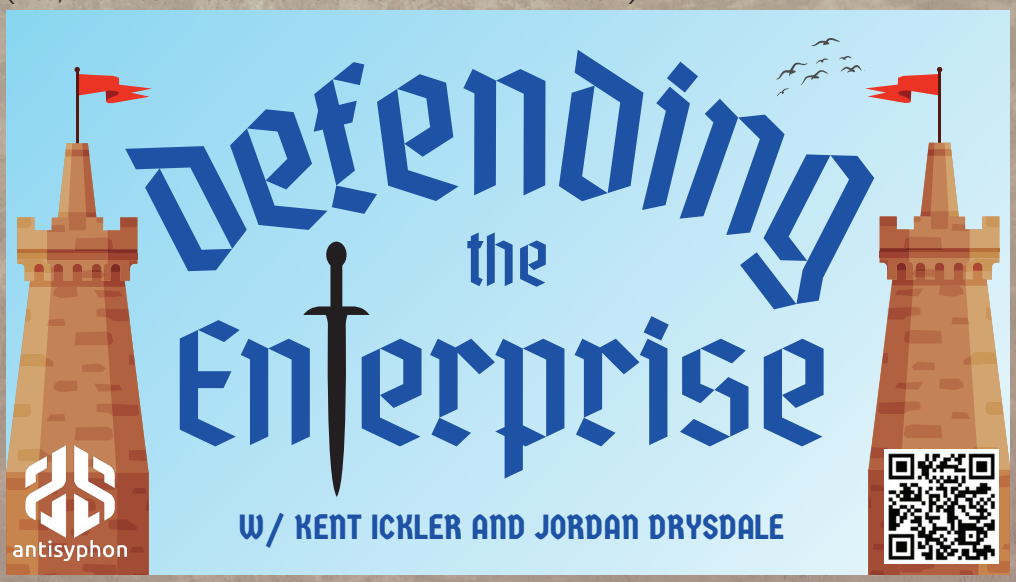
Olaf Hartong
Sysmon-modular
https://github.com/olafhartong/sysmon-modular

JPCert
LogonTracer
https://github.com/JPCERTCC/LogonTracer

Tool Analysis Result Sheet
https://jpcertcc.github.io/ToolAnalysisResultSheet/

BHIS
EventLogging
https://github.com/blackhillsinfosec/EventLogging

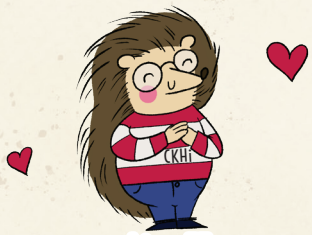
(Also, check out this awesome class from Kent and Jordan!)



"LETTERS" TO THE EDITOR(s)

DEAR EDITOR:
Thank you very much for the super interesting, highly informative, and entertaining magazine. You are doing an admirable, mega great job! ... and yes the comic is simply great, funny ... but in the end I had tears in my eyes. What a great, wonderful woman and mother! I take my hat off to you.
Michael S. from Düsseldorf, Germany

You've got us all blushing over here, Michael. Comments like this are what keep us going.



chinno53

DEAR EDITOR:
As a Blue Teamer, I particularly like the "Pen Tester's Tears" page, which describes times that Blue Teams have scuppered Red Teamer's plans.
Ste W. from Warrington, England

I think we all like to feel better about ourselves by laughing at someone else's misery sometimes.

DEAR EDITOR:
"The new phone book is here! The new phone book is here!" Thanks Black Hills Information Security, John Strand, and crew... it was like Christmas came early when I opened my mailbox.
Gregory from Des Moines, Iowa

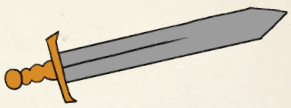
Careful, Greg, you're showing your age. (But also, Merry Christmas).

DEAR EDITOR:
Mail call from Black Hills Information Security – Prompt# Magazine plus some Backdoors and Breaches cards and a sticker? Some real nostalgic vibes here. My wife is laughing at me going through my loot here. Since this is #1 though should I open it or put it on EBay in 20 years?
Tony Z. from Denver, Colorado

I was convinced to keep the tags on my Beanie Babies when I was a kid and I hated it. But you do you... and remember me when you're a thousandaire in 20 years.

DEAR EDITOR:
Thank you from the bottom of my heart for all that you do for the infosec community. BHIS is one of the main reasons why I (a female) felt comfortable enough entering this field in the first place. Keep up the amazing work you all are doing. I look forward to seeing your future successes.
Candace H. from Tracy, California

That's high praise, Candace! Hearing feedback like this is why I (also a female) love what I do at BHIS and will keep doing it. Keep being awesome and beating up that status quo.



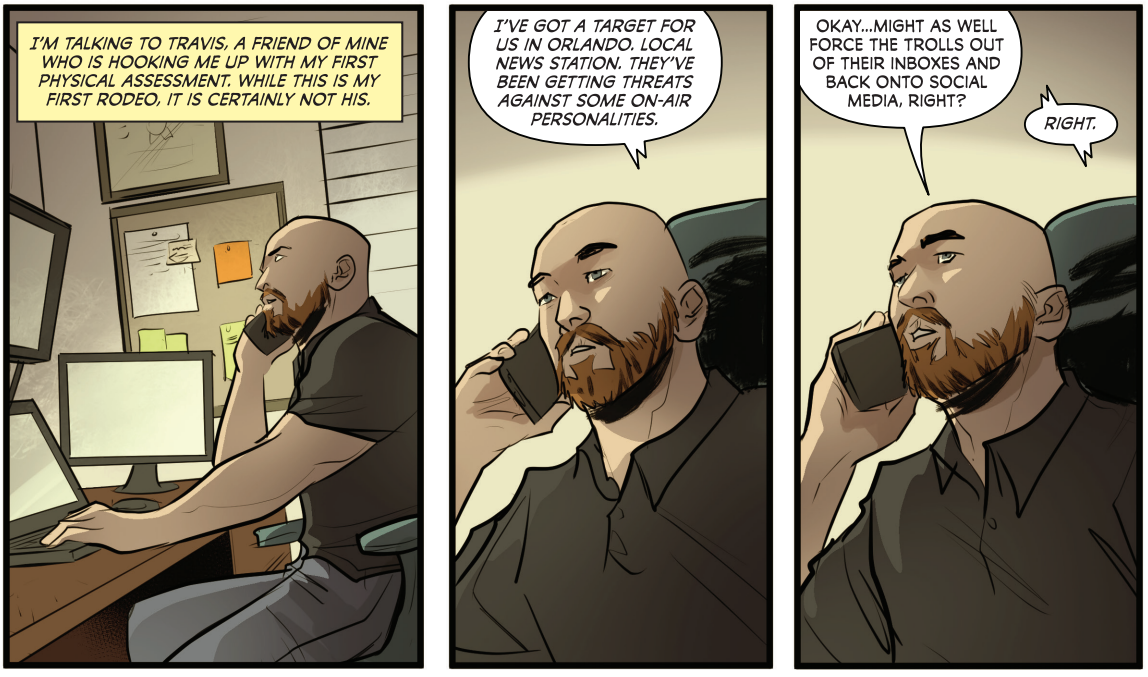
DEAR EDITOR:
How much will the print version cost? I just want to make sure I budget for this in the new year, as I will gladly give you folks all my bottle caps (will 2,240 per year cover it?)
Paul B. from Edmonton, Alberta

We may be living in a post- (currently?) apocalyptic world, Paul, but we still don't want your money. Send me a Nuka-Cola and we'll call it even.

DEAR EDITOR:
When I grow up, I want to be BHIS! Love what you all are doing for the community.
Darius H. from the United States of America

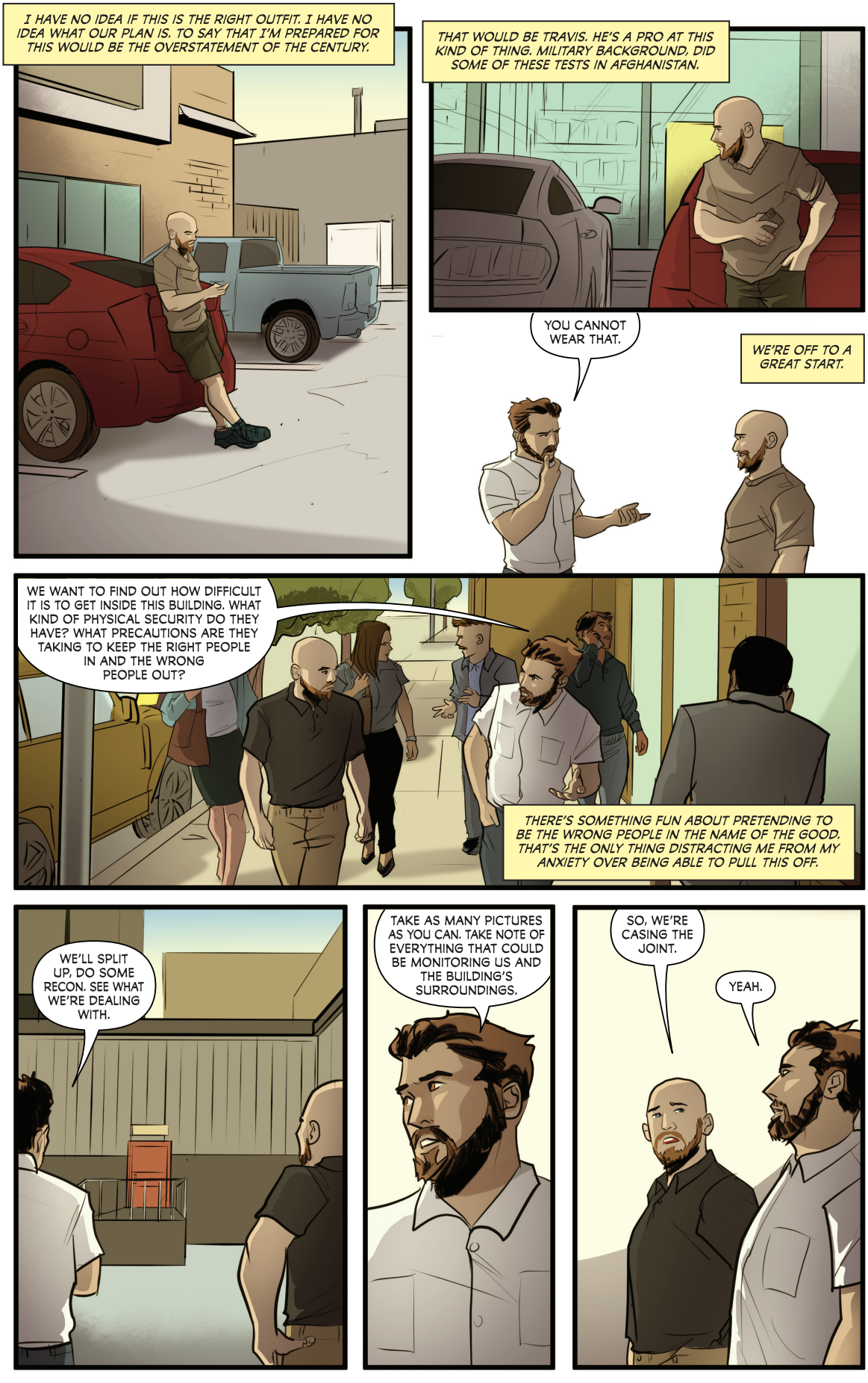
Just be the best you; nobody else. At least, that's what my mom says.

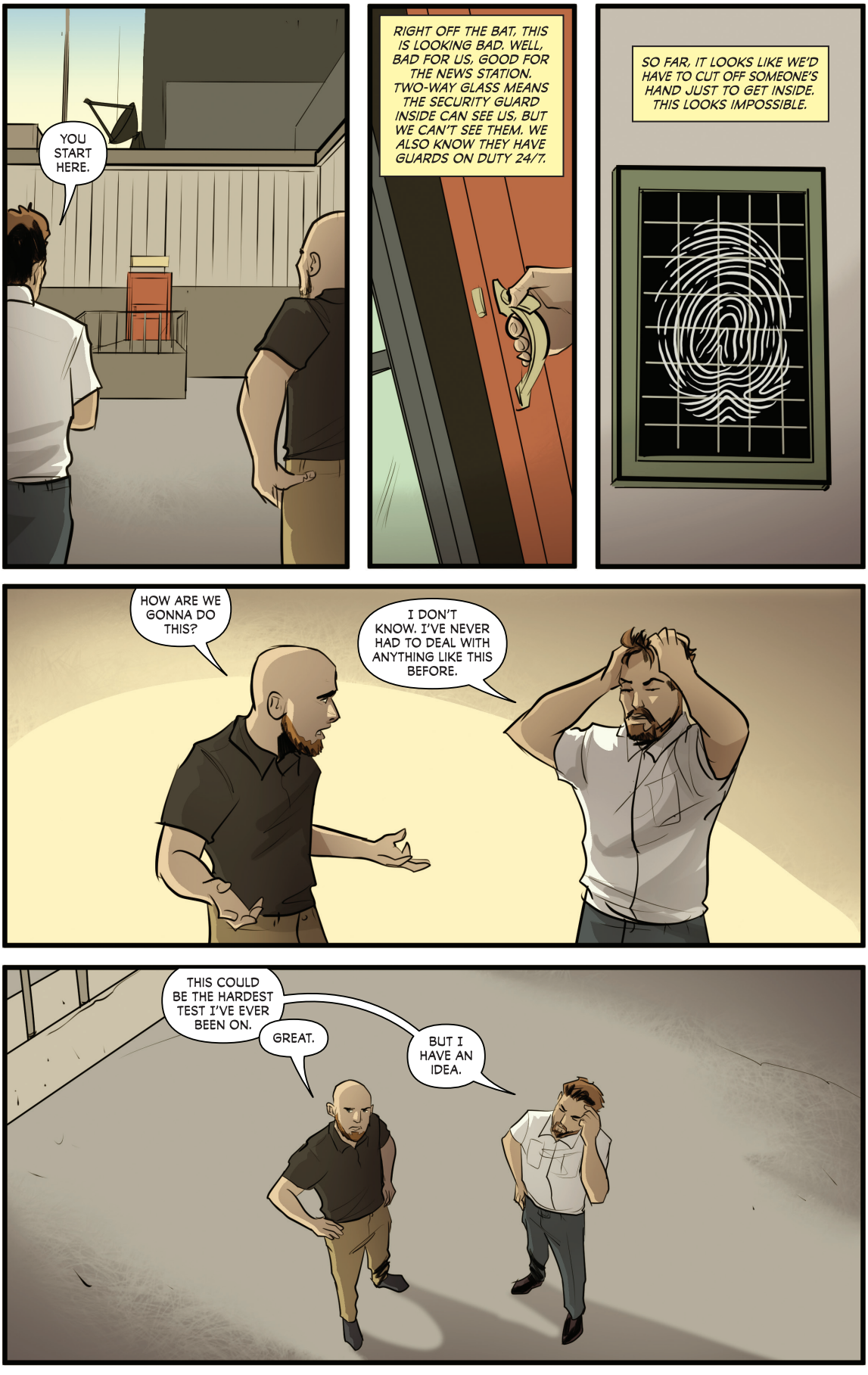
We really love what we get to do, and your encouragement is the fuel that keeps us running.
You can always share your thoughts with us at info@promptzine.com!

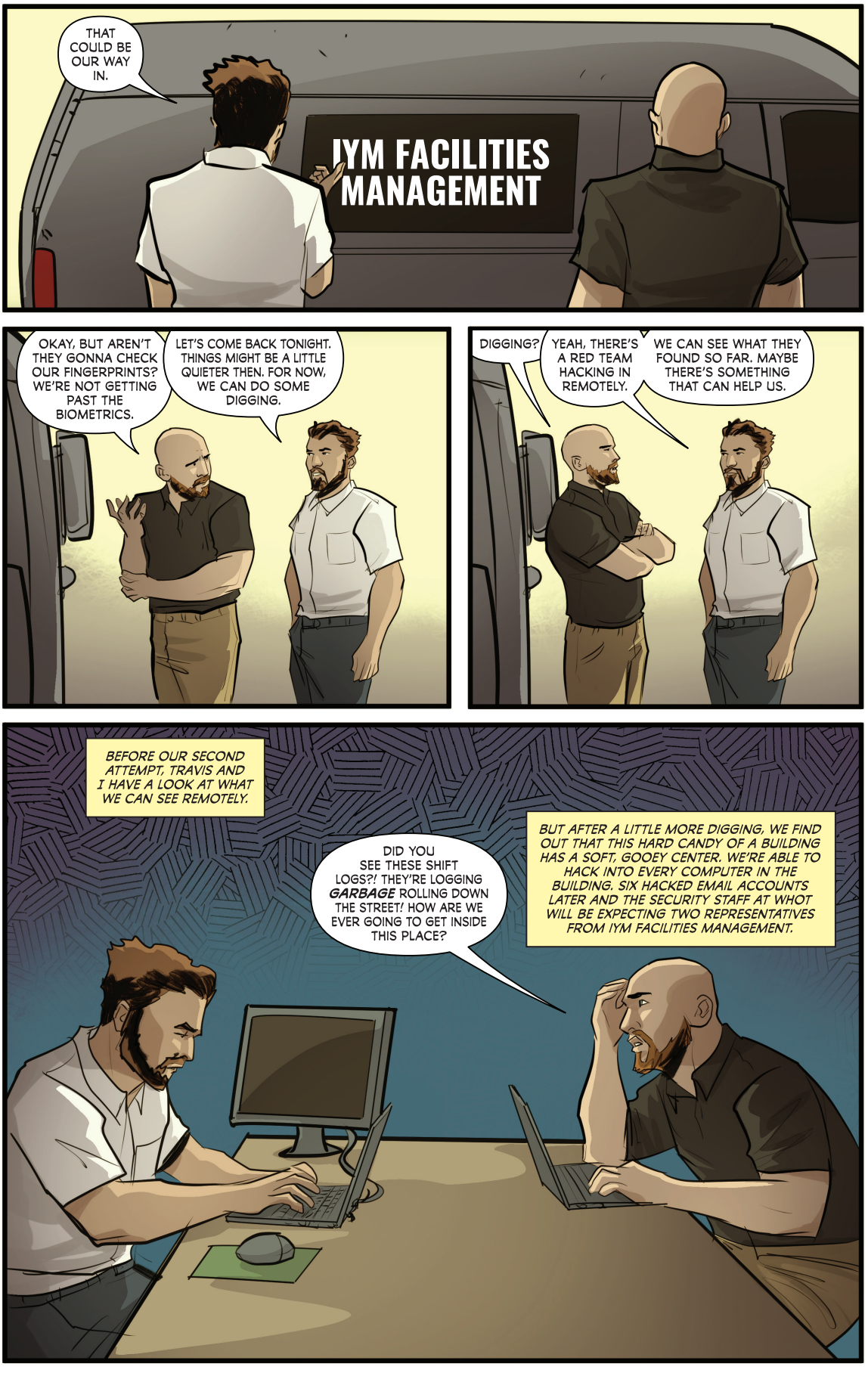


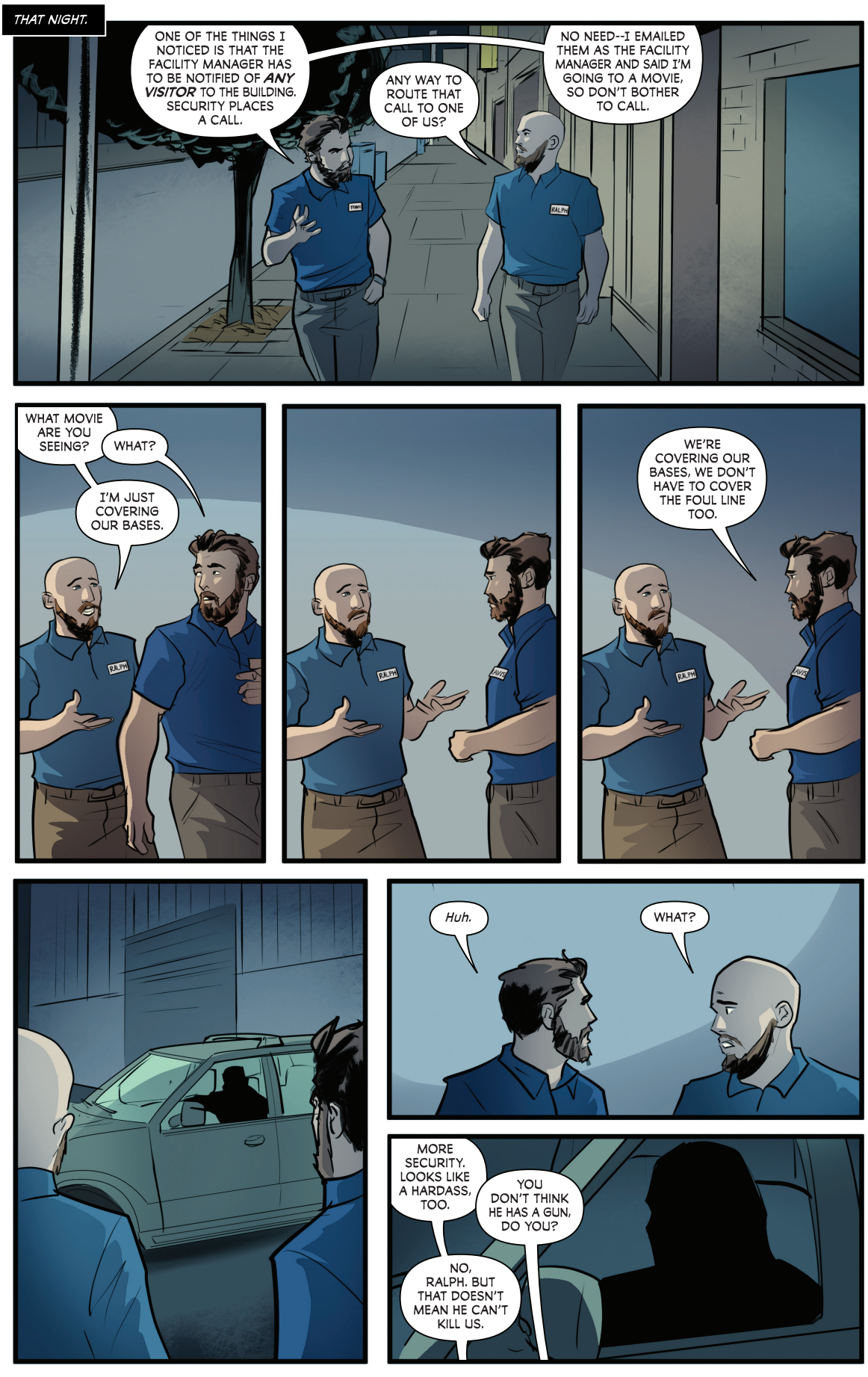
An Unlikely Alliance:
Inspired by True Events

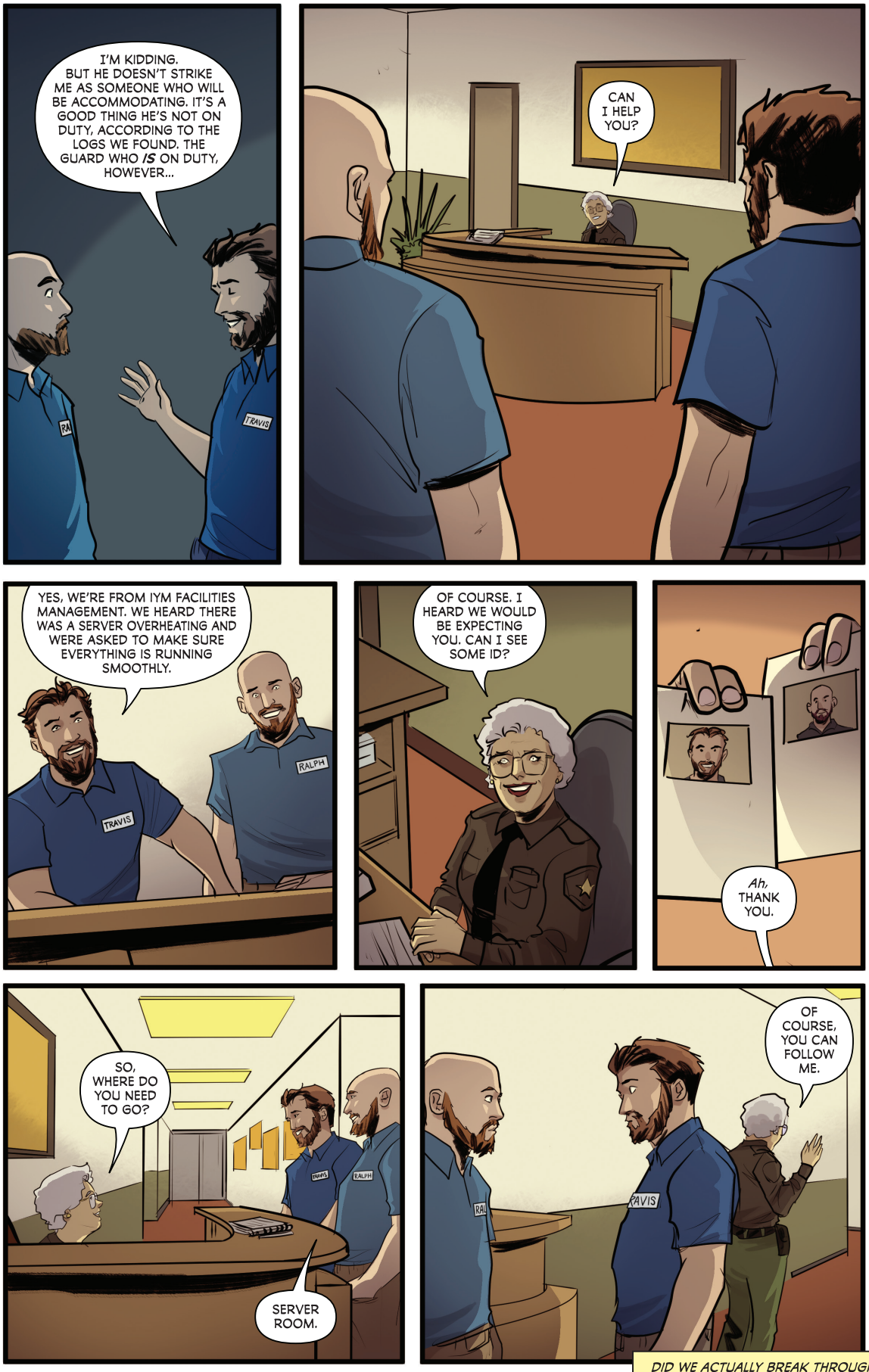
ORIGINAL STORY: Ralph May (@ralphte1)
WRITER: Jamie Frevele (@jamiefrevele)
ARTIST: Joe Eisma (@supajoe)
COLORIST: Shari Chankhamma (@sharihes)
LETTERER: Taylor Esposito (@tayloresposo)
EDITOR: Kassie Kimball (@sneaky_space)

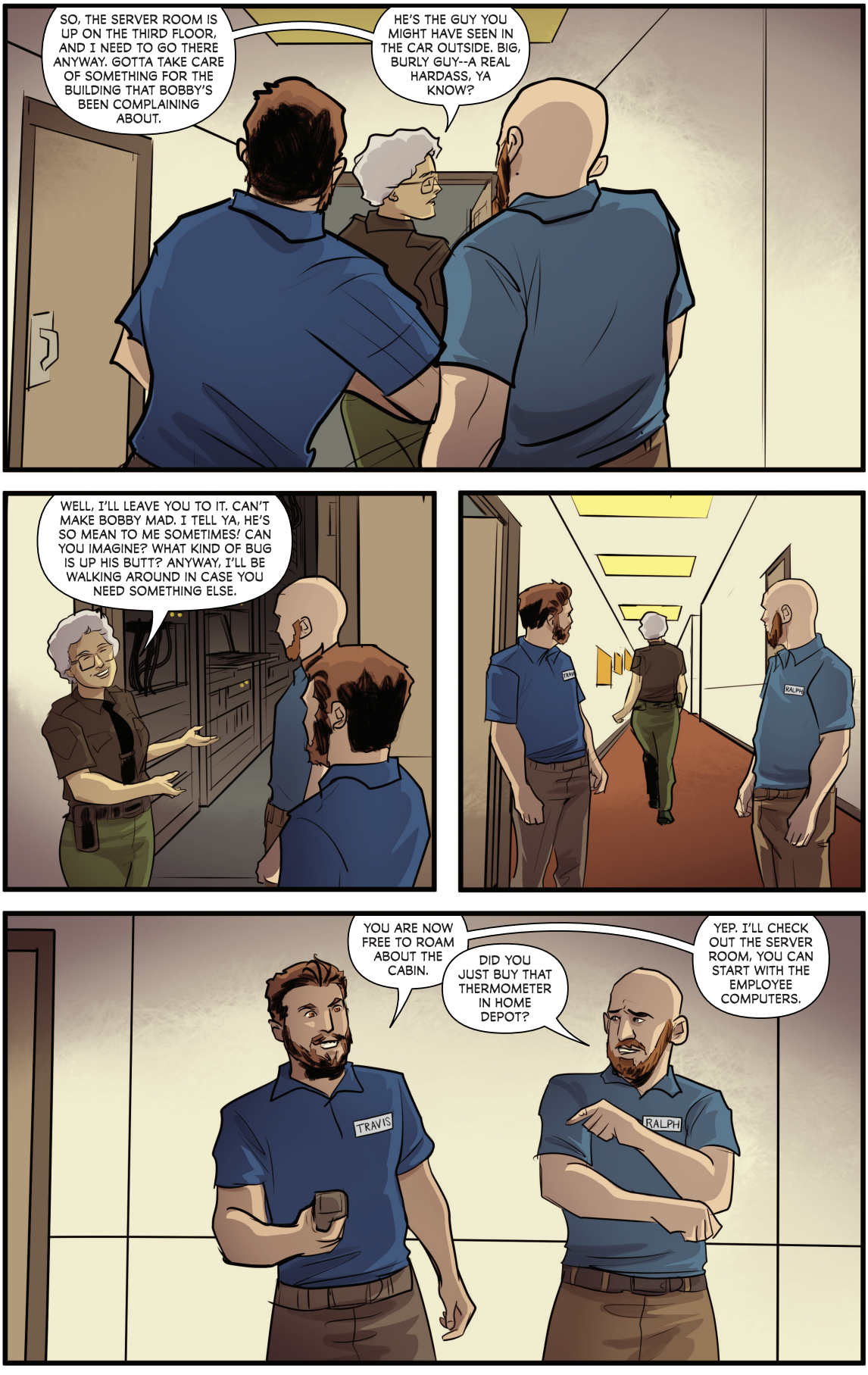

I HAVE NO IDEA IF THIS IS THE RIGHT OUTFIT. I HAVE NO IDEA WHAT OUR PLAN IS. TO SAY THAT I'M PREPARED FOR THIS WOULD BE THE OVERSTATEMENT OF THE CENTURY.
THAT WOULD BE TRAVIS. HE'S A PRO AT THIS KIND OF THING. MILITARY BACKGROUND, DID SOME OF THESE TESTS IN AFGHANISTAN.
YOU CANNOT WEAR THAT.
WE'RE OFF TO A GREAT START.
WE WANT TO FIND OUT HOW DIFFICULT IT IS TO GET INSIDE THIS BUILDING. WHAT KIND OF PHYSICAL SECURITY DO THEY HAVE? WHAT PRECAUTIONS ARE THEY TAKING TO KEEP THE RIGHT PEOPLE IN AND THE WRONG PEOPLE OUT?
THERE'S SOMETHING FUN ABOUT PRETENDING TO BE THE WRONG PEOPLE IN THE NAME OF THE GOOD. THAT'S THE ONLY THING DISTRACTING ME FROM MY ANXIETY OVER BEING ABLE TO PULL THIS OFF.
WE'LL SPLIT UP, DO SOME RECON. SEE WHAT WE'RE DEALING WITH.
TAKE AS MANY PICTURES AS YOU CAN. TAKE NOTE OF EVERYTHING THAT COULD BE MONITORING US AND THE BUILDING'S SURROUNDINGS.
SO, WE'RE CASING THE JOINT.
YEAH.

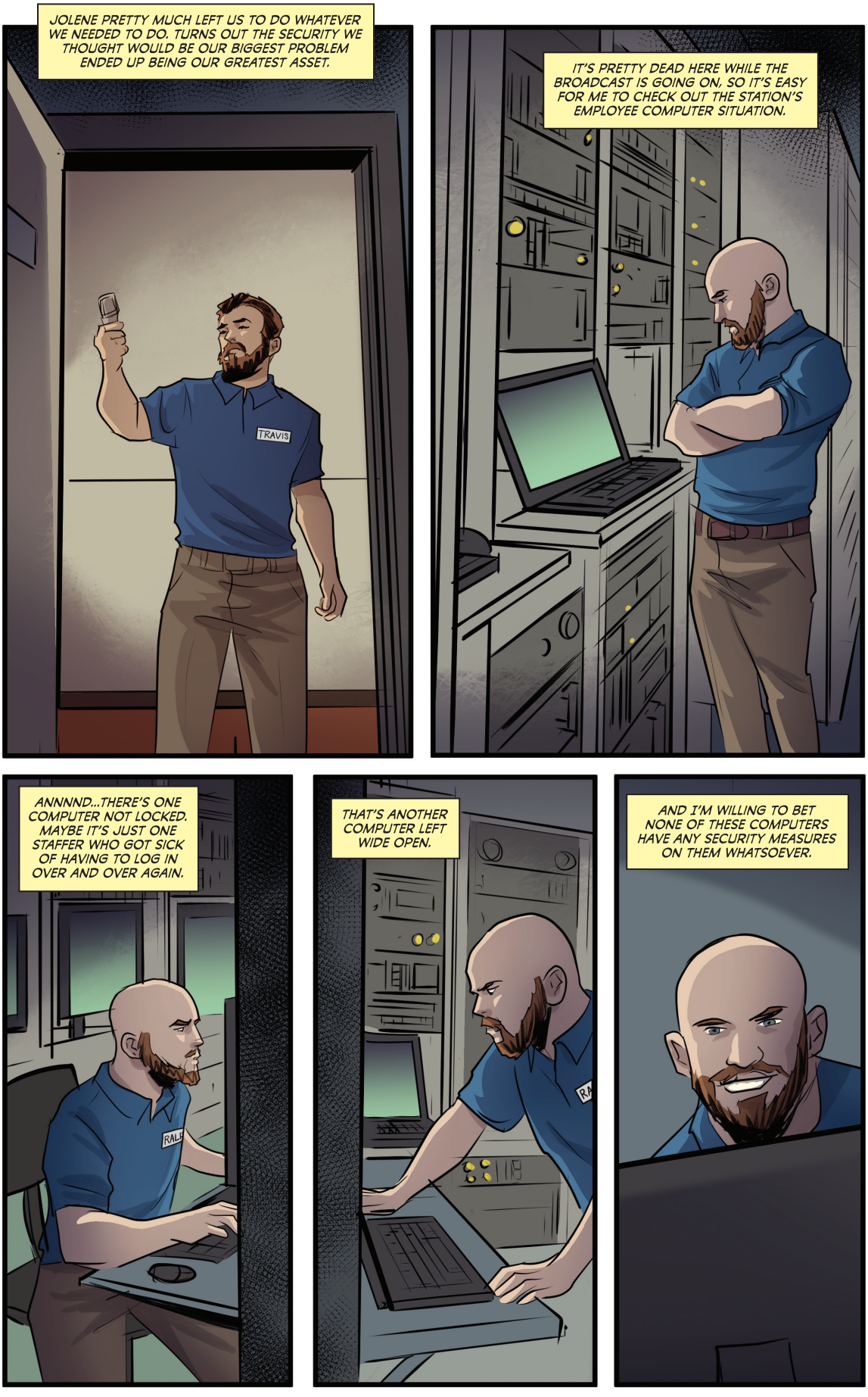

YOU START HERE.
RIGHT OFF THE BAT, THIS IS LOOKING BAD. WELL, BAD FOR US, GOOD FOR THE NEWS STATION. TWO-WAY GLASS MEANS THE SECURITY GUARD INSIDE CAN SEE US, BUT WE CAN'T SEE THEM. WE ALSO KNOW THEY HAVE GUARDS ON DUTY 24/7.
SO FAR, IT LOOKS LIKE WE'D HAVE TO CUT OFF SOMEONE'S HAND JUST TO GET INSIDE. THIS LOOKS IMPOSSIBLE.
HOW ARE WE GONNA DO THIS?
I DON'T KNOW. I'VE NEVER HAD TO DEAL WITH ANYTHING LIKE THIS BEFORE.
THIS COULD BE THE HARDEST TEST I'VE EVER BEEN ON.
GREAT.
BUT I HAVE AN IDEA.

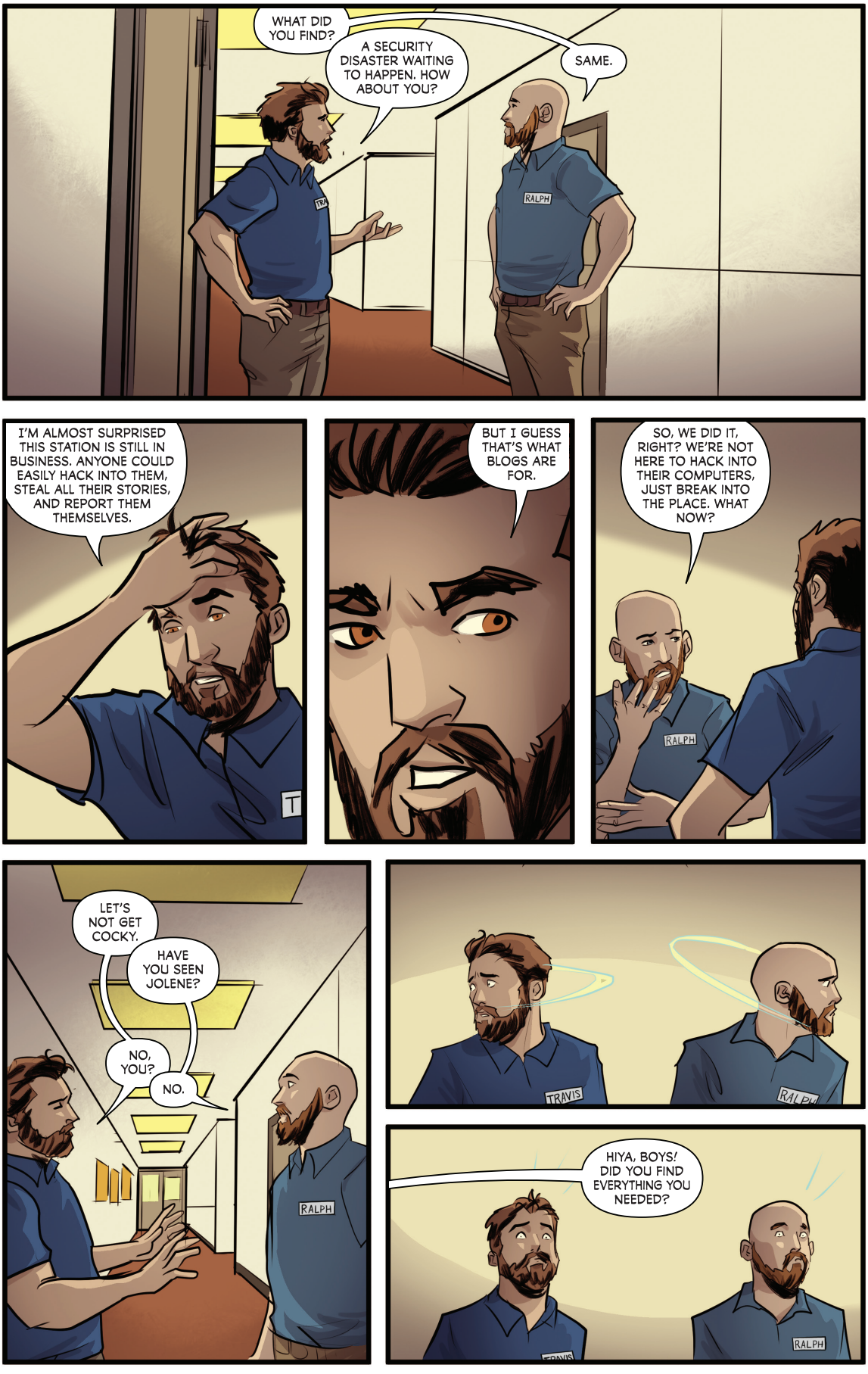

THAT COULD BE OUR WAY IN.
IYM FACILITIES MANAGEMENT
OKAY, BUT AREN'T THEY GONNA CHECK OUR FINGERPRINTS? WE'RE NOT GETTING PAST THE BIOMETRICS.
LET'S COME BACK TONIGHT. THINGS MIGHT BE A LITTLE QUIETER THEN. FOR NOW, WE CAN DO SOME DIGGING.
DIGGING?
YEAH, THERE'S A RED TEAM HACKING IN REMOTELY.
WE CAN SEE WHAT THEY FOUND SO FAR. MAYBE THERE'S SOMETHING THAT CAN HELP US.
BEFORE OUR SECOND ATTEMPT, TRAVIS AND I HAVE A LOOK AT WHAT WE CAN SEE REMOTELY.
DID YOU SEE THESE SHIFT LOGS?! THEY'RE LOGGING GARBAGE ROLLING DOWN THE STREET! HOW ARE WE EVER GOING TO GET INSIDE THIS PLACE?
BUT AFTER A LITTLE MORE DIGGING, WE FIND OUT THAT THIS HARD CANDY OF A BUILDING HAS A SOFT, GOOEY CENTER. WE'RE ABLE TO HACK INTO EVERY COMPUTER IN THE BUILDING. SIX HACKED EMAIL ACCOUNTS LATER AND THE SECURITY STAFF AT WHOT WILL BE EXPECTING TWO REPRESENTATIVES FROM IYM FACILITIES MANAGEMENT.

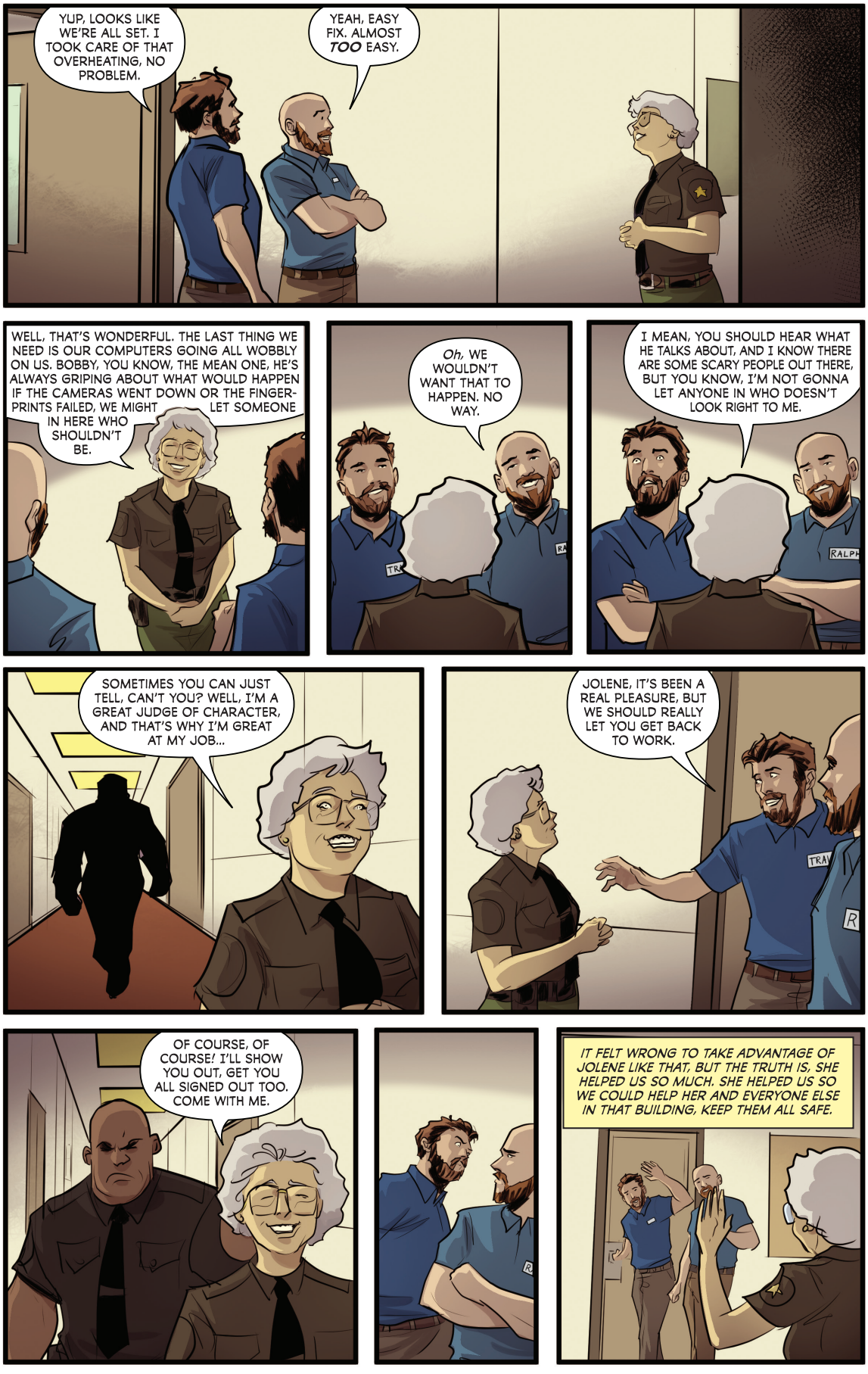

THAT NIGHT.
ONE OF THE THINGS I NOTICED IS THAT THE FACILITY MANAGER HAS TO BE NOTIFIED OF ANY VISITOR TO THE BUILDING. SECURITY PLACES A CALL.
ANY WAY TO ROUTE THAT CALL TO ONE OF US?
NO NEED--I EMAILED THEM AS THE FACILITY MANAGER AND SAID I'M GOING TO A MOVIE, SO DON'T BOTHER TO CALL.
RALPH
WHAT MOVIE ARE YOU SEEING?
WHAT?
I'M JUST COVERING OUR BASES.
RALPH
RALPH
LAVIS
WE'RE COVERING OUR BASES, WE DON'T HAVE TO COVER THE FOUL LINE TOO.
RALPH
LAVIS
Huh.
WHAT?
MORE SECURITY. LOOKS LIKE A HARDASS, TOO.
YOU DON'T THINK HE HAS A GUN, DO YOU?
NO, RALPH. BUT THAT DOESN'T MEAN HE CAN'T KILL US.

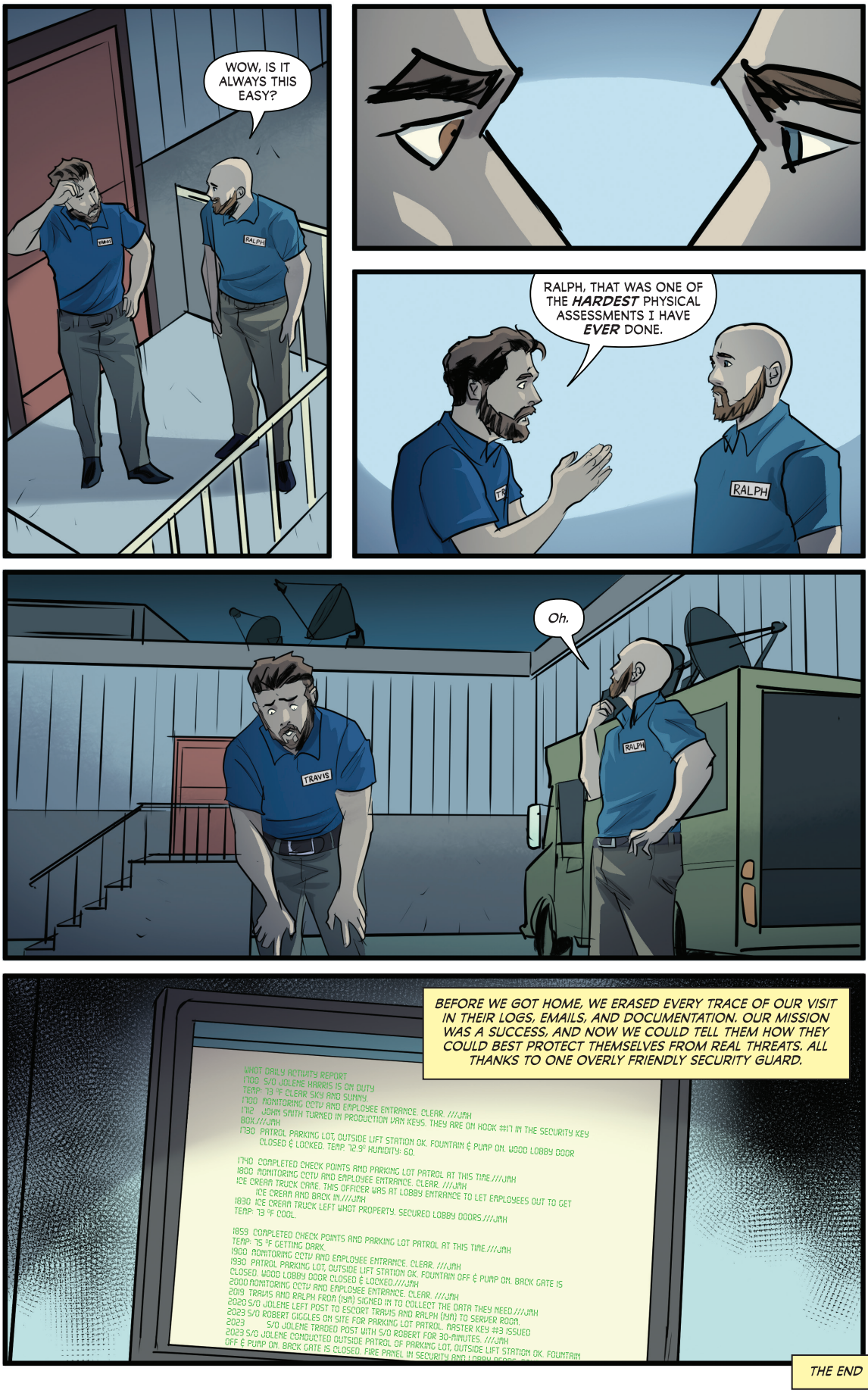

I'M KIDDING. BUT HE DOESN'T STRIKE ME AS SOMEONE WHO WILL BE ACCOMMODATING. IT'S A GOOD THING HE'S NOT ON DUTY, ACCORDING TO THE LOGS WE FOUND. THE GUARD WHO *IS* ON DUTY, HOWEVER...
TRAVIS
CAN I HELP YOU?
YES, WE'RE FROM IYM FACILITIES MANAGEMENT. WE HEARD THERE WAS A SERVER OVERHEATING AND WERE ASKED TO MAKE SURE EVERYTHING IS RUNNING SMOOTHLY.
TRAVIS
RALPH
OF COURSE. I HEARD WE WOULD BE EXPECTING YOU. CAN I SEE SOME ID?
Ah, THANK YOU.
SO, WHERE DO YOU NEED TO GO?
SERVER ROOM.
OF COURSE, YOU CAN FOLLOW ME.
DID WE ACTUALLY BREAK THROUGH TO THE GOOEY CENTER...THAT EASILY?

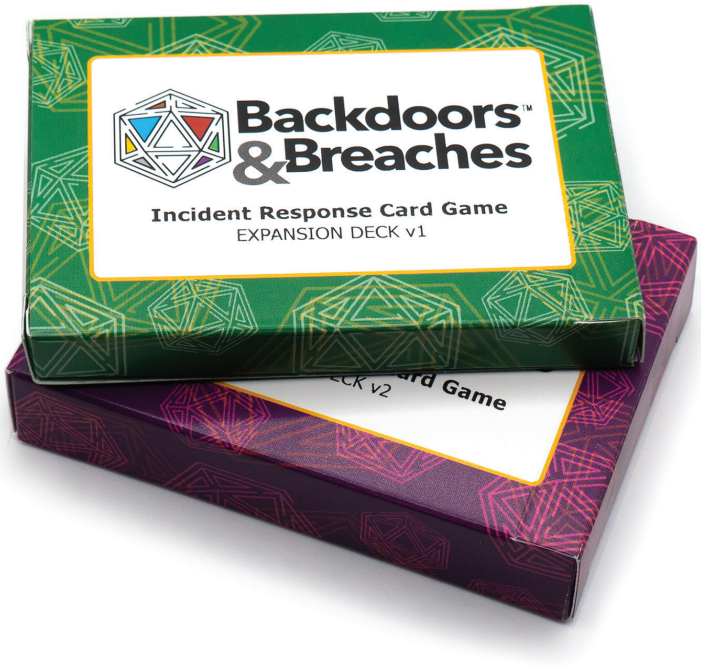

SO, THE SERVER ROOM IS UP ON THE THIRD FLOOR, AND I NEED TO GO THERE ANYWAY. GOTTA TAKE CARE OF SOMETHING FOR THE BUILDING THAT BOBBY'S BEEN COMPLAINING ABOUT.
HE'S THE GUY YOU MIGHT HAVE SEEN IN THE CAR OUTSIDE. BIG, BURLY GUY--A REAL HARDASS, YA KNOW?
WELL, I'LL LEAVE YOU TO IT. CAN'T MAKE BOBBY MAD. I TELL YA, HE'S SO MEAN TO ME SOMETIMES! CAN YOU IMAGINE? WHAT KIND OF BUG IS UP HIS BUTT? ANYWAY, I'LL BE WALKING AROUND IN CASE YOU NEED SOMETHING ELSE.
TRAVIS
RALPH
YOU ARE NOW FREE TO ROAM ABOUT THE CABIN.
DID YOU JUST BUY THAT THERMOMETER IN HOME DEPOT?
YEP. I'LL CHECK OUT THE SERVER ROOM, YOU CAN START WITH THE EMPLOYEE COMPUTERS.
TRAVIS
RALPH


JOLENE PRETTY MUCH LEFT US TO DO WHATEVER WE NEEDED TO DO. TURNS OUT THE SECURITY WE THOUGHT WOULD BE OUR BIGGEST PROBLEM ENDED UP BEING OUR GREATEST ASSET.
TRAVIS
IT'S PRETTY DEAD HERE WHILE THE BROADCAST IS GOING ON, SO IT'S EASY FOR ME TO CHECK OUT THE STATION'S EMPLOYEE COMPUTER SITUATION.
ANNNND...THERE'S ONE COMPUTER NOT LOCKED. MAYBE IT'S JUST ONE STAFFER WHO GOT SICK OF HAVING TO LOG IN OVER AND OVER AGAIN.
THAT'S ANOTHER COMPUTER LEFT WIDE OPEN.
AND I'M WILLING TO BET NONE OF THESE COMPUTERS HAVE ANY SECURITY MEASURES ON THEM WHATSOEVER.


WHAT DID YOU FIND?
A SECURITY DISASTER WAITING TO HAPPEN. HOW ABOUT YOU?
SAME.
RALPH
I'M ALMOST SURPRISED THIS STATION IS STILL IN BUSINESS. ANYONE COULD EASILY HACK INTO THEM, STEAL ALL THEIR STORIES, AND REPORT THEM THEMSELVES.
BUT I GUESS THAT'S WHAT BLOGS ARE FOR.
SO, WE DID IT, RIGHT? WE'RE NOT HERE TO HACK INTO THEIR COMPUTERS, JUST BREAK INTO THE PLACE. WHAT NOW?
RALPH
LET'S NOT GET COCKY.
HAVE YOU SEEN JOLENE?
NO, YOU?
NO.
RALPH
TRAVIS
HIYA, BOYS! DID YOU FIND EVERYTHING YOU NEEDED?
RALPH


YUP, LOOKS LIKE WE'RE ALL SET. I TOOK CARE OF THAT OVERHEATING, NO PROBLEM.
YEAH, EASY FIX. ALMOST *TOO* EASY.
WELL, THAT'S WONDERFUL. THE LAST THING WE NEED IS OUR COMPUTERS GOING ALL WOBBLY ON US. BOBBY, YOU KNOW, THE MEAN ONE, HE'S ALWAYS GRIPING ABOUT WHAT WOULD HAPPEN IF THE CAMERAS WENT DOWN OR THE FINGERPRINTS FAILED, WE MIGHT LET SOMEONE IN HERE WHO SHOULDN'T BE.
Oh, WE WOULDN'T WANT THAT TO HAPPEN. NO WAY.
I MEAN, YOU SHOULD HEAR WHAT HE TALKS ABOUT, AND I KNOW THERE ARE SOME SCARY PEOPLE OUT THERE, BUT YOU KNOW, I'M NOT GONNA LET ANYONE IN WHO DOESN'T LOOK RIGHT TO ME.
SOMETIMES YOU CAN JUST TELL, CAN'T YOU? WELL, I'M A GREAT JUDGE OF CHARACTER, AND THAT'S WHY I'M GREAT AT MY JOB...
JOLENE, IT'S BEEN A REAL PLEASURE, BUT WE SHOULD REALLY LET YOU GET BACK TO WORK.
OF COURSE, OF COURSE! I'LL SHOW YOU OUT, GET YOU ALL SIGNED OUT TOO. COME WITH ME.
IT FELT WRONG TO TAKE ADVANTAGE OF JOLENE LIKE THAT, BUT THE TRUTH IS, SHE HELPED US SO MUCH. SHE HELPED US SO WE COULD HELP HER AND EVERYONE ELSE IN THAT BUILDING, KEEP THEM ALL SAFE.


WOW, IS IT ALWAYS THIS EASY?
TRAVIS
RALPH
RALPH, THAT WAS ONE OF THE HARDEST PHYSICAL ASSESSMENTS I HAVE EVER DONE.
RALPH
Oh.
TRAVIS
RALPH
BEFORE WE GOT HOME, WE ERASED EVERY TRACE OF OUR VISIT IN THEIR LOGS, EMAILS, AND DOCUMENTATION. OUR MISSION WAS A SUCCESS, AND NOW WE COULD TELL THEM HOW THEY COULD BEST PROTECT THEMSELVES FROM REAL THREATS. ALL THANKS TO ONE OVERLY FRIENDLY SECURITY GUARD.
WHOT DAILY ACTIVITY REPORT
1100 S/O JOLENE HARRIS IS ON DUTY
TEMP: 73 °F CLEAR SKY AND SUNNY.
1700 MONITORING CCTV AND EMPLOYEE ENTRANCE. CLEAR. ///JAH
1712 JOHN SMITH TURNED IN PRODUCTION VAN KEYS. THEY ARE ON HOOK #17 IN THE SECURITY KEY BOX.///JAH
1730 PATROL PARKING LOT, OUTSIDE LIFT STATION OK. FOUNTAIN & PUMP ON. WOOD LOBBY DOOR CLOSED & LOCKED. TEMP: 72.9° HUMIDITY: 60.
1740 COMPLETED CHECK POINTS AND PARKING LOT PATROL AT THIS TIME.///JAH
1800 MONITORING CCTV AND EMPLOYEE ENTRANCE. CLEAR. ///JAH
ICE CREAM TRUCK CAME. THIS OFFICER WAS AT LOBBY ENTRANCE TO LET EMPLOYEES OUT TO GET ICE CREAM AND BACK IN.///JAH
1830 ICE CREAM TRUCK LEFT WHOT PROPERTY. SECURED LOBBY DOORS.///JAH
TEMP: 73 °F COOL
1859 COMPLETED CHECK POINTS AND PARKING LOT PATROL AT THIS TIME.///JAH
TEMP: 75 °F GETTING DARK.
1900 MONITORING CCTV AND EMPLOYEE ENTRANCE. CLEAR. ///JAH
1930 PATROL PARKING LOT, OUTSIDE LIFT STATION OK. FOUNTAIN OFF & PUMP ON. BACK GATE IS CLOSED. WOOD LOBBY DOOR CLOSED & LOCKED.///JAH
2000 MONITORING CCTV AND EMPLOYEE ENTRANCE. CLEAR. ///JAH
2019 TRAVIS AND RALPH FROM (IVA) SIGNED IN TO COLLECT THE DATA THEY NEED.///JAH
2020 S/O JOLENE LEFT POST TO ESCORT TRAVIS AND RALPH (IVA) TO SERVER ROOM.
2023 S/O ROBERT GIGGLES ON SITE FOR PARKING LOT PATROL. MASTER KEY #3 ISSUED
2023 S/O JOLENE TRADED POST WITH S/O ROBERT FOR 30-MINUTES. ///JAH
2023 S/O JOLENE CONDUCTED OUTSIDE PATROL OF PARKING LOT, OUTSIDE LIFT STATION OK. FOUNTAIN OFF & PUMP ON. BACK GATE IS CLOSED. FIRE PANEL IN SECURITY AND LOBBY DOORS
THE END



SPEARPHISH GENERAL STORE

[do you trust us?]