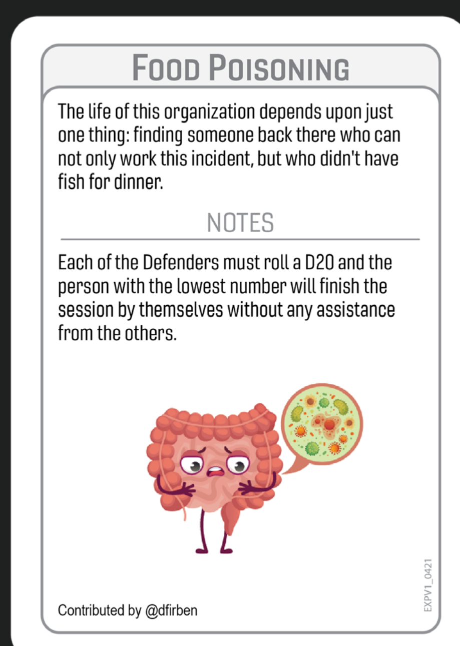
PROMPT#

Prompt
Zine
~~Choose~~
~~Wisely~~
Black
Hills
Information
Security

R11: 1 3 2 1 1 1 1 2



PROMPT#

R18: 1 1 1 1 1 2 1

Check out some MUSIC TO HACK TO by our very own **Beau Bullock:**

NOBANDWIDTH

https://www.nobandwidth.io/

CREDITS

Publisher: John Strand
@strandjs

Editor-in-Chief: Jason Blanchard
@BanjoCrashland

Designer & Illustrator: Anna Hughes
annahughesdesign.myportfolio.com

Associate Editor: Deb Wigley
@debthedeb

Copy Editor: Kassie Kimball
linkedin.com/in/kassiekimball

Cover Artist: Scott Saslow
scottsaslow.com

Escape Room Engineer: Ben Korbelak

Tool Shed Editor: Marcello Salvati
@byt3bl33d3r

Coloring Contest Artist: Alessandro Micelli
instagram.com/themicellis

Comic Book: *A White Hat for Rita*

Writer/Editor: Jamie Frevele
@jamiefrevele

Artist: Joe Eisma
@Supajoe

Colorist: Shari Chankhamma
https://sharii.com/

Letterer: Taylor Esposito
@TaylorEspo

Art Contributors: Giulia Gualazzi, Alex Owens, Bradley Samuelson & Alessandro Micelli

1 4 2 3 *CHOOSE WISE-LY#

C18: 1 1 1 2 1

If you need a unique password,
Use a phrase.
Then add a symbol and number,
for some praise.
Passphrases are much stronger,
Especially if they are longer.
An example is:
1 super cool passphrase!

-- @Infosec_Taylor

INTRO

Proudly Sucking At Capitalism

When starting a company, at some point, you need to figure out what kind of company you want to have. To be honest, this is easy for several people in the industry. You just follow the template. Start a company, do something, then look for investors or some type of "exit." When my wife and I started BHIS, this was not the path we wanted to go down. So, we set out doing our own thing, on our own terms.

A large number of the things we have done do not fit into the paths, goals, and objectives many VC exit strategy findings companies follow. For example, creating an IR card game and promptly giving it away for free, doing Pay What You Can Training (PWYC), doing webcast after webcast after webcast and never selling the attendees' info out to vendors.

This is what we mean by saying that we are "proudly sucking at capitalism." We are keeping our focus on people: our employees, our customers, and our community - not profits. We focus on maximizing what we give to the community and not asking what our return on investment is. We don't hate capitalism; we hate how many companies play it. Focusing on profits at all costs is not fun and morally exhausting so we decided to set out and create a new path, a new template.

And we did.

What you are holding in your hands is another crazy, fun idea of BHIS. No profit goals. No ROI calculations. Just bringing together a bunch of cool stories, poetry, and games in a comic is a dream come true. It also does not make a whole lot of sense from a business perspective. Darn near giving it away makes even less sense. But, if you truly want to own something, give it away. It will be yours forever.

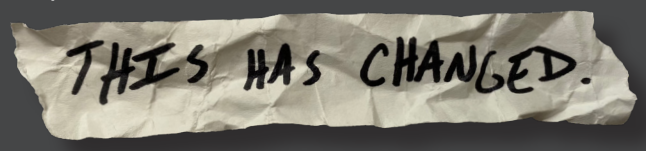
Erica and John

C22: 1 3 1 2 6 1

BREACHING the CLOUD

by Beau Bullock

Flashback only 10 years and you would see a drastic change in how companies manage their computing resources. Chilled datacenters in dark corners of office buildings housed critical infrastructure to protect it from external threat actors. Visualizing where your crown jewels are and how to get to them was a lot easier back then. Most orgs would take a "tower defense" approach to protect sensitive data and critical assets on-premises behind a firewall.



"The cloud" has enabled businesses to grow in ways they could not before. Instead of employees connecting to an on-prem network with VPN to use things like email, intranet sites, and perform daily tasks, they are now leveraging productivity suites that are 100% cloud-based.

Instead of running a physical server in a datacenter, that same server is now running on a virtual instance in the cloud. Instead of storing large databases or files on physical hard drives, that data is now being stored in cloud-based storage buckets. Instead of defending one tower, organizations now have multiple towers to defend

that are spread across the globe (using a cloud provider's infrastructure) and can be accessed in many ways via public application programming interface (API).

As organizations have evolved how they run their infrastructure, so too have our penetration testing methodologies evolved. **When it comes to initial access, phishing has been king for many years.** A close second to that would be password-based attacks. Both of these attacks look different now due to cloud usage. I used to focus my efforts on finding an externally-exposed Outlook Web Access (OWA) server, as this was a very common webmail tool used by many organizations. OWA, along with VPNs and other externally-exposed authentication portals that leveraged Active Directory-based authentication, were prime targets for password spraying. Now, that focus has shifted towards cloud-based services such as Microsoft 365.

Microsoft 365 has changed the way that many businesses manage email. This, in effect, means that instead of targeting an on-prem OWA server, we are now targeting Microsoft 365 services directly. Getting access to an employee's Microsoft 365 account typically means access to not only email (Outlook), but also SharePoint, Teams, OneDrive, and more.

I was on a red team engagement for a large financial institution where due to some cloud-based misconfigurations, I was able to remotely compromise their network. After successfully password spraying one of their employees at the Microsoft 365 Outlook portal, I found they had Multi-Factor Authentication (MFA) enabled on the account. This prevented me from logging into the user's email with a web browser. As mentioned earlier, most cloud services have additional APIs. Azure has one called the Microsoft Graph API. I tried authenticating to this API with the sprayed user's credentials and, sure enough, I was authenticated and bypassed the need for the user's MFA. The Graph API allows for reading the Azure Active Directory user list. What this enabled me to do was extract the full username list for the organization where I had previously only had a partial list built during reconnaissance.

I took the full list, which had thousands more users than I previously had, and started password spraying again. With the full user list, I ended up spraying many more accounts. In testing out authentication for these accounts, I found that some had not yet enrolled in the MFA product used by the company. So I enrolled for them. This now allowed me to authenticate to the Outlook portal with a web browser. In addition to being able to read their email, I could also view what they had permission to read on SharePoint. Their SharePoint site provided details on what was needed to VPN into the network, including the client certificate needed for authentication. I installed the client certificate on a virtual machine and successfully connected over VPN to their network.

Inconsistencies in MFA deployments is one of the bigger trends I have seen when it comes to cloud-based misconfigurations.

Conditional access policies allow organizations to enable fine-grained controls over how users authenticate. These can range from the location a user is authenticating from, the device they are using, and also if they are trying to access legacy portals. Because of these inconsistencies, I wrote a tool to check for potential single-factor access on Microsoft services that I call MFASweep: https://github.com/dafthack/MFASweep

Once you compromise a set of credentials, checking for MFA inconsistencies can be done by importing the MFASweep PowerShell script and running the following command (substituting the credentials):

```
Invoke-MFASweep
-Username:
targetuser@targetdomain.com
-Password: Winter2021
```

There is a big difference between utilizing the cloud for "productivity" tools vs. "infrastructure." Services like Microsoft 365 or Google Workspace enable employees to be productive with things like email, shared drives, chat, and document editing tools. While these are technically "cloud-hosted" services, they are separate from the infrastructure side where virtual machines, databases, web applications, serverless technologies, and more can be spun up. In fact, they have separate APIs in most cases for communicating with them.

More organizations are using cloud services for infrastructure instead of hosting systems in their own datacenters. As a penetration tester or red teamer assessing this infrastructure, you must look at these resources from a different angle. What do you do after you get access to an Amazon AWS access key ID and secret access key? If you compromise a Microsoft Azure user who has a subscription, what can you access? How do you pivot in the cloud? These are some of the questions that over the last few years I have needed to answer out of necessity due to facing them head-on. I have collected what I have learned into a training course that I call "Breaching the Cloud."

This course serves as my own personal methodology that I reference when performing assessments involving any aspect of "the cloud."

In my opinion, we are just scratching the surface of organizations leveraging cloud resources. In addition to the rapid deployment of critical business infrastructure to the cloud, these services themselves are evolving daily. Organizations are still learning new ways to configure access, security protections, and alerting. These, along with completely new services being established altogether, will create a higher potential for security issues to arise in the future.

R10: 3 3 3 1 1 1

CHECK OUT Beau's *"Breaching the Cloud"* Training Course!
wildwesthackinfest.com

C23: 1 3 1 1 2 1 1 2

"Within one environment that I was testing, the organization had configured their service accounts in such a way that they could only log on to specific systems and they could not authenticate from the network to those systems. They did this because they could not change the weak passwords to those service accounts. Because they were service accounts with weak passwords, we could Kerberoast and crack their passwords. However, despite having administrative access to several machines, those credentials were completely worthless to us during testing. It was very disheartening, to say the least."

David Fletcher, BHIS Tester

"I was testing a very old, very hand-written webapp. I found a command injection vulnerability that allowed me to read and write files on the web server. I found and downloaded the source code files to see if I could find credentials and the hostname for the database server. Then I uploaded a web shell, connected, and... the connection broke and I couldn't communicate with the web server anymore. I thought maybe I'd crashed something. Then my phone rang. Now I was sure I had crashed something. But nope. The blue team had noticed a cmd.exe spawned from IIS and knew that should never happen. They'd shut me down and were calling to gloat."

BB King, BHIS Tester

"One time on a red team assessment, I got burned before I ever sent any phishing emails, simply by registering a domain. The target company tracked doppelgänger domains that used their company's name as part of the domain. They were alerted to the registration of the domain and immediately redirected all email from that domain to their SOC. None of our phishing emails ever reached the target's inboxes, which completely killed the campaign."

Beau Bullock, BHIS Tester

C14: 1 1 2 2 2

R8: 1 2

Community Leaders

A note from debthedeb:

Here at Black Hills Information Security, we think of our community as part of our family, and the backbone of that family is our Community Leaders. You can find them throughout our Discord servers answering questions, giving advice, and being all-around fantastic humans. I'd like to introduce you to one of them!

MEET @KADAWI!

1. When/Why/How did you get started in Security?

I am just getting started! I'm actually a convert from graphic design into security. I stumbled upon some ethical hacking courses several years ago and they hooked me. Since then, I have been pursuing a Master's in Cybersecurity, where I have been lucky enough to serve as president of our student-run cybersecurity research lab, as well as work as a teaching assistant for our offensive security class. I can't wait to make the jump from academics into solving real world problems.

2. Are you choosing to focus on the red or blue team?

I don't know how anyone can choose. Red and blue are both so essential and cool (for lack of a better word)! I am blown away by the creativity of exploits and defenses. Would I rather use things in unexpected ways to bend systems to my will (maybe a little dramatic), or put on my Sherlock Holmes hat and tie all the pieces together to stop the bad guys? I want to do it all!

3. What's the most frustrating thing about security?

From my perspective, I am really irked by people and companies capitalizing on the buzzword of "cybersecurity" in disingenuous ways. There is always someone touting their magical solution and false promises to solve all your problems. Or someone getting paid to speak pretty words that feel good but are actually meaningless and not actionable. Or someone claiming they want to "close the skills gap" by offering overpriced training that pumps out students who are still unprepared for the jobs they want.

4. What's the most encouraging thing about security?

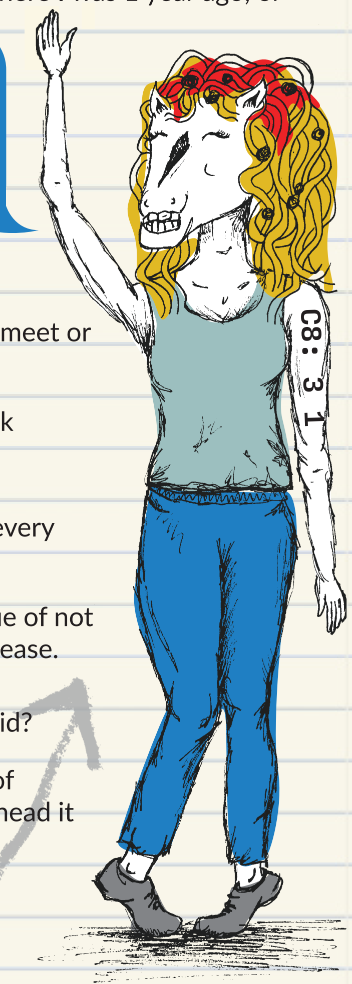
The people. I am in awe of the selflessness of many of the people and communities in security. There are many unsung heroes out there. People who help for the sake of helping. People who give you a glimpse into the goodness of humanity. The more of that we have, the better.

R21: 1 3 1 1 6 1

5. Why do you like helping lead the Black Hills Infosec Community?

See previous answer about selfless communities. I am lucky that BHIS has allowed me the opportunity to be involved in their communities. As I said before, I am not a seasoned veteran of security, but helping lead the Black Hills community gives me the opportunity to use where I am now to help others who are where I was 1 year ago, or 3 years ago.

"Too often beginners are made to feel ashamed for their lack of knowledge, and I love that this community is a place where people can come to learn and be supported. I am happy to be a part of that."



C8: 3 1

6. Would you rather...?

Q. Would you rather be compelled to high-five everyone you meet or be compelled to give wedgies to anyone in a green shirt?

A. High fives, all the way. High fives make people feel like rock stars. They always put a smile on someone's face.

Q. Would you rather have edible spaghetti hair that regrows every night or sweat maple syrup?

A. My wee ones love pancakes. They have taught me the value of not being covered in maple syrup. I'll take the spaghetti hair, please.

Q. Would you rather be a reverse centaur or a reverse mermaid?

A. Fish head or horse head? The ocean is a beautiful place… of terrors, so I'm not sure I'd cut it down there. I guess horse head it is. At least I'll have nice hair.

We'd like to invite you to be a part of our community, your new 3rd place.

C11: 2 4 2 1 2 2

VISIT HTTPS://DISCORD.GG/BHIS

ATLANTIC CITY ATTRIBUTION

BY JOHN STRAND

cyber deception

cyber deception

I was in Atlantic City for a computer forensic conference where I had gotten in late... very late. Like, 4 hours of sleep then present in the morning. I honestly do not remember much of anything about the presentation except that I was working on a forensics gig at the time and some of the more "interesting" pictures from a report ended up being displayed on the screen. That is a different story for another time.

After I was done presenting, I immediately went to my room and crashed. I had no idea what time it was, and, honestly, I did not care.

At about 12-ish AM, I received a call from a friend of mine working with law enforcement. I was groggy and disoriented and had to take a few moments to get my bearings and figure out where I was.

'Crap, I am in Atlantic City,' I thought as the person on the other end of the line was panic-dumping what was clearly important information about a case he was working. Unfortunately for him, trying to get any information through to me at the time was kind of like playing tennis against curtains.

As the fog was lifting, the story I was hearing was crystallizing as my brain struggled to get into gear.

There was a little girl, about 9, that was abducted, and law enforcement wanted to see if there were any "hacking" tricks we could use to get the location of the suspect. We knew he had the girl; he had changed his Skype icon to a picture of her crying face. We also had an acquaintance who was willing to work with us and communicate with the suspect over Skype.

This was back in the day when Skype was very much unwilling to work with law enforcement to obtain user location information, even with a warrant.

The question was simple: Was there a way to get location information by sending something to the suspect?

In fact, there was. As part of penetration testing, we often track the number of users that open documents we send as part of phishing campaigns. Documents have been excellent attack vectors for years. As testers, we use them all the time by inserting various malicious payloads in the form of macros.

However, we did not have authorization to get full access to the suspect's system. We just wanted locational data. That's it.

To do this, we needed to use a project called Word Web Bugs.

www.blackhillsinfosec.com/tag/web-word-bugs/

This project utilizes the insertion of references to images and CSS data into a Word document. However, the actual content is hosted on another server owned by the good guys. The trick is collecting the IP address of the system, the timestamp, and the source port. While geolocation based on IP address is difficult, with the IP address, timestamp, and source port, you generally have enough information for an ISP to track the actual location down with a properly executed warrant.

BUT HOW DOES THIS WORK?

Let's look at the code.

As you can see at the top of the next page, the code appears to be HTML. Which is weird. But what many people do not know is that

```
<html>
<head>
<LINK REL="stylesheet" HREF="http://YOUR_IP/web-bug-server/index.php?id=1&type=css"></head>
<body>
<p>What a buggy document!</p>
<IMG SRC= "http://YOUR_IP/web-bug-server/index.php?id=1&type=img" width="1" height="1">
</body>
</html>
```

Word (and many other document editors) are actually very lightweight browsers. Basically, the code you see above is not what you would type into Word, but rather is the code you would create with a lower-level editor like vi. When Word opens the document, it attempts to render the HTML and in doing so, it fires the request for the CSS data and the image source tag.

On the backend, the database receives the connection. As you can see below, this works with a number of different editors.

type	ip address	user agent	
img	127.0.0.1	gvfs/1.12.1	AbiWord
css	127.0.0.1	LibreOffice Writer	
img	127.0.0.1		
img	192.168.1.195	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko)	Apple TextEdit
css	192.168.1.195	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko)	
css	192.168.1.216	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727	Microsoft Word
img	192.168.1.216	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727	

With this technology, we inserted the tracking elements into the document along with a news story about the missing girl. Then the acquaintance started a Skype chat with the suspect and, after a lot of conversation, was able to send the document with the tracking elements to the suspect. After about ten minutes, the suspect opened the document and the callback triggered. Once we had the IP address, timestamp, and source port, we were able to get a warrant and quickly got the girl back.

I say "we" although I did very little of the actual work. I was directing and helping law enforcement set up their servers and create the document. In all reality, after the server and the file were set up, I said "good luck" and went back to bed.

I did not hear that the plan was successful till months afterwards. The outstanding men and women of law enforcement, working together with various judges and the people at the ISP, were the ones on the ground level who made this happen. This is a success story due to their hard work and dedication. I am grateful and honored that I was able to help in my own small way.

You can help too. Please go to **missingkids.org/HOME** to donate and be part of the solution.

To find out how to use the technique in this story, please check out our Active Defense & Cyber Deception class via the link below:

https://wildwesthackinfest.com/antisyphon//active-defense-cyber-deception-john-strand/

C12: 9 1 1

RED TEAM ING–

A STORY FROM THE TRENCHES

by Joff Thyer

C16: 2 3 1 2 1 4

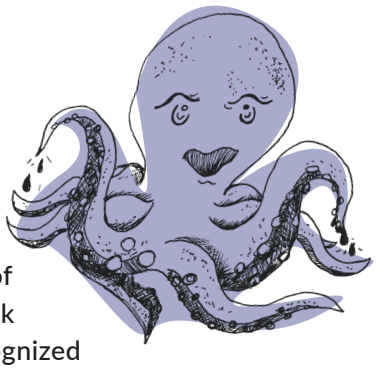
I remember a day when a customer (now a friend) bragged that the deployed application allowlisting policies at his organization were highly secure, thorough, and well vetted. Naturally, I asked about the process he undertook to create such a thing. My friend replied, "We started by considering all of the Microsoft Windows operating systems and applications to be hostile. Everything was blocked and we built from the ground up."

I have to say that I was intrigued. How many organizations would live through the pain of application allowlisting on steroids, an approach that blocked everything and then selectively allowed only what is needed, including the operating system itself? For a little context, we have had a relationship with our friend for a number of years. At the start of our customer relationship, this person asked the right questions. In response, we literally posed: "DO YOU WANT TO TAKE THE RED PILL, OR THE BLUE PILL?" He chose red and began a program to build some of the most robust defenses that he possibly could.

Zoom forward a few years into this relationship and we graduated to a full-blown red team exercise, as many in our industry would think appropriate. Coming into the red teaming exercise, I and my teammate Ethan had decided that we really wanted to gain physical access to the organization and implant a command channel on the first machine we encountered. We began our preparations in earnest and reached the point of considering what command channel we wanted to implant.

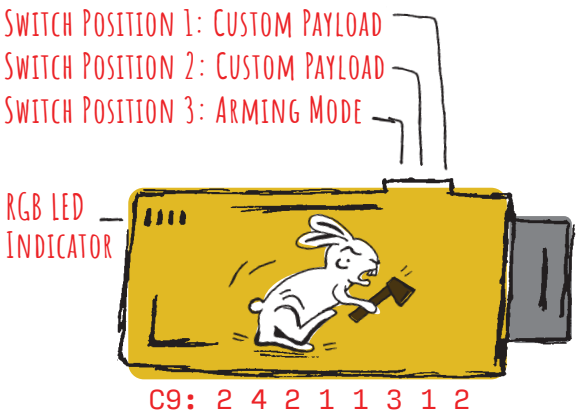
What could we do? There was no possibility of running any binary content, any visual basic scripts, macros, PowerShell, and/or commands on these systems. We knew just how much the program had developed and had been locked down hard. To give a little more context, we are speaking of running our operations in early 2017. A lot of the current application allowlisting bypasses that are fairly widely published now were not really public knowledge.

As I was researching around the Internet for application allowlisting bypasses, I came across a few Twitter posts from @subTee and, having encountered some of his materials before, began to get interested in the techniques that were published mostly as GitHub gists. What caught my attention was an attack that leveraged the REGSVR32.EXE binary, which in turn would load the Windows scripting runtime DLL named "scrobj.dll" to execute a block of Jscript. This attack became well recognized by the moniker "SquiblyDoo" around that same time period.



From my perspective though, I found the need to fetch a script object from an external resource to be unnecessary, so I decided to modify the attack. I authored some code I later called "WEvade" (I am not good at naming) which used the same technique as SquiblyDoo but implemented in a custom DLL that did not attempt to interpret any form of script. Instead, the attack read the required shellcode from a file or web server and directly executed base64 encoded shellcode contained within that file or URL.

After we tested and ensured that the custom malware would successfully evade antivirus solutions and application allowlisting, we began preparing for our physical incursion! Between Ethan and I, we geared up with a Bash Bunny and USB stick as backup, just in case the Bash Bunny failed for any reason.



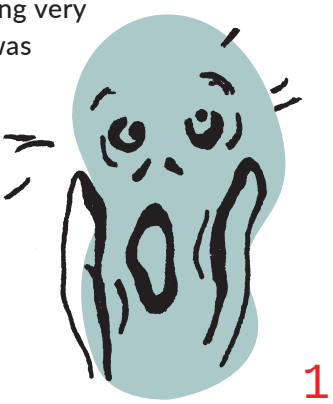
C9: 2 4 2 1 1 3 1 2

The Bash Bunny is a fun hacker gadget that has a small Debian Linux installation on it, and can present itself as USB storage or a human keyboard interface device for the express delivery of malware payloads!

Finally, the day had arrived for our adventure. Ethan and I nervously pulled up to a parking meter on the street next to the target organization premises. We both had all of the gear in hand, and cellular modems for communications to the command channel infrastructure.

In these situations, there is always that nervous sort of moment when you have the discussion that goes along the lines of "OK, WHO IS GOING TO ATTEMPT TO ENTER THE PREMISES AND DO THE NERVE-WRACKING PART OF THE WORK?" I managed to convince Ethan to do that part of the exercise, so he grabbed his bag and set out for the lobby. As it turns out, this was a multi-tenant and multi-floor building, so Ethan literally picked someone who looked like an employee that might work at the organization and followed them into the elevator. Later, we discovered that Ethan had actually hitched a ride up the elevator with the company CEO, making small talk all the way up.

Ethan quickly found out that getting off at the correct floor allowed him direct access to the organization, so he walked casually into the door and found the nearest computer workstation, immediately whipping out the Bash Bunny and plugging it in. Ethan then discovered that the organization's policies did not allow human interface-style devices to be connected, so he reverted to a USB storage method. He also had trouble with this mechanism and began getting very nervous as he was an unknown face messing around with a computer workstation in a pretty open office setting!



The following SMS transaction between us then transpired whereby Ethan asked me to quickly deploy a web server with the payload files on it. The funniest part of the entire SMS transaction is when I realized that Ethan did not just want a web server, but a web server WITH THE PAYLOAD FILES on it. I have been accused of being "too literal" in the past. This time it was along the lines of anxiety-driven stupidity. See the SMS right here:

ETHAN: "[IT'S] GIVING ME INDEX.HTML"

JOFF: "YES THAT'S RIGHT. YOU WANT SOMETHING ELSE??"

Ethan definitely must have thought I had either lost my mind completely or was playing a really poorly-timed joke.

CAN YOU START A WEB SERVER AND SEND ME THE IP

STANDBY

138.197.112.155

OUR NGINX BOX

PATH?

JUST ROOT... /VAR/WWW/HTML

GIVING ME INDEX.HTML

YES THATS RIGHT. YOU WANT SOMETHING ELSE??

I NEED THE DLL AND PAYLOAD

OK.
MY DLL RIGHT?

THE PAYLOADS USB ISN'T WORKING

JUST SERVE THE PAYLOADS DIR ON THE CALLBACK SYSTEM

PYTHON HTTPSERVER

DONE

HIT SAME URL

WHAT'S THE PAYLOAD NAME?

SOMETHING SIMPLE OTHER

PLEASE

HIT IT AGAIN

ITS PYTHON NOW

DIR INDEXING IS WORKING

PORT 80?

NVM

SHELL

WOOT!

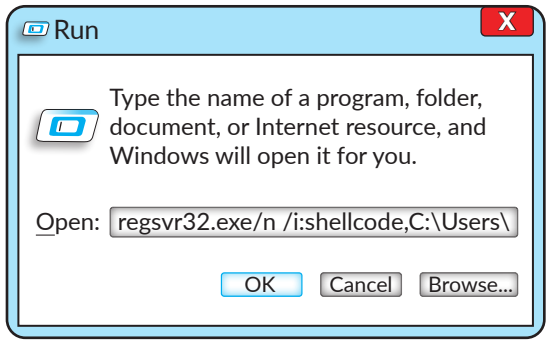
I'M WORKING ON SCREENSHOTS

EXCELLENT

Near Hysterical and Rapid Pace Red Teamer SMS Exchange in the Heat of Battle

It worked! We got a command channel fully operational, and I did my customary "root dance" in the driver seat of my rental vehicle downstairs.

As we later in the day were regaling our success, celebrating mightily that we had bested the application allowlisting deployment, our point of contact and friend told us that he almost succeeded in stopping us.



Application Allowlisting Bypass in Motion

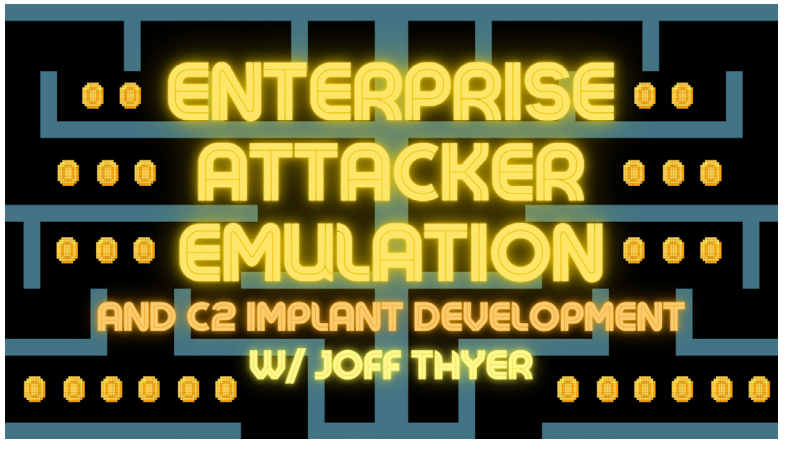
Of course, we were feeling pretty cocky by that time and asked how that could be possible. I mean, we had won that first hurdle of gaining a foothold! As it so happens, our customer had an interesting solution deployed that detected whenever any USB storage device was connected to one his workstations. The defense solution had indeed done its job and alerted the system administrator in his office that an unknown USB device had been connected to this workstation.

Being very security conscious, the alert system administrator made his way upstairs to the workstation cubicle area to find out what was going on. As he was on his way, he needed a quick bathroom break, by which time Ethan had already succeeded and had hightailed his way out of the office pronto! Amusingly, Ethan even ran into the system administrator on his way out, giving quick eye contact and trying to continue looking casual while leaving the scene.

I suppose that the moral of the story is that, "WHEN YOU GOTTA GO, WELL YOU JUST GOTTA GO, RIGHT?" Who would have known that a penetration tester (aka threat actor) had just run in the door and dropped a malware payload, only to exit stage left and somehow completely avoid revealing his purpose by virtue of lucky timing?! As was also discovered later, it was fortuitous that Ethan even found an unoccupied workstation without the screen being locked. So ends this tale from the Red Teaming trenches where, by a combination of skill and sheer luck, we bested the people, process, and technology literally by seconds and, of course, had a great deal of fun and laughs afterwards.

C15: 1 5 1 1 1 1 1 1 1

R23: 1 3 1 2 1 1 2 1 1



C24: 1 1 1 1 1 1 2 1

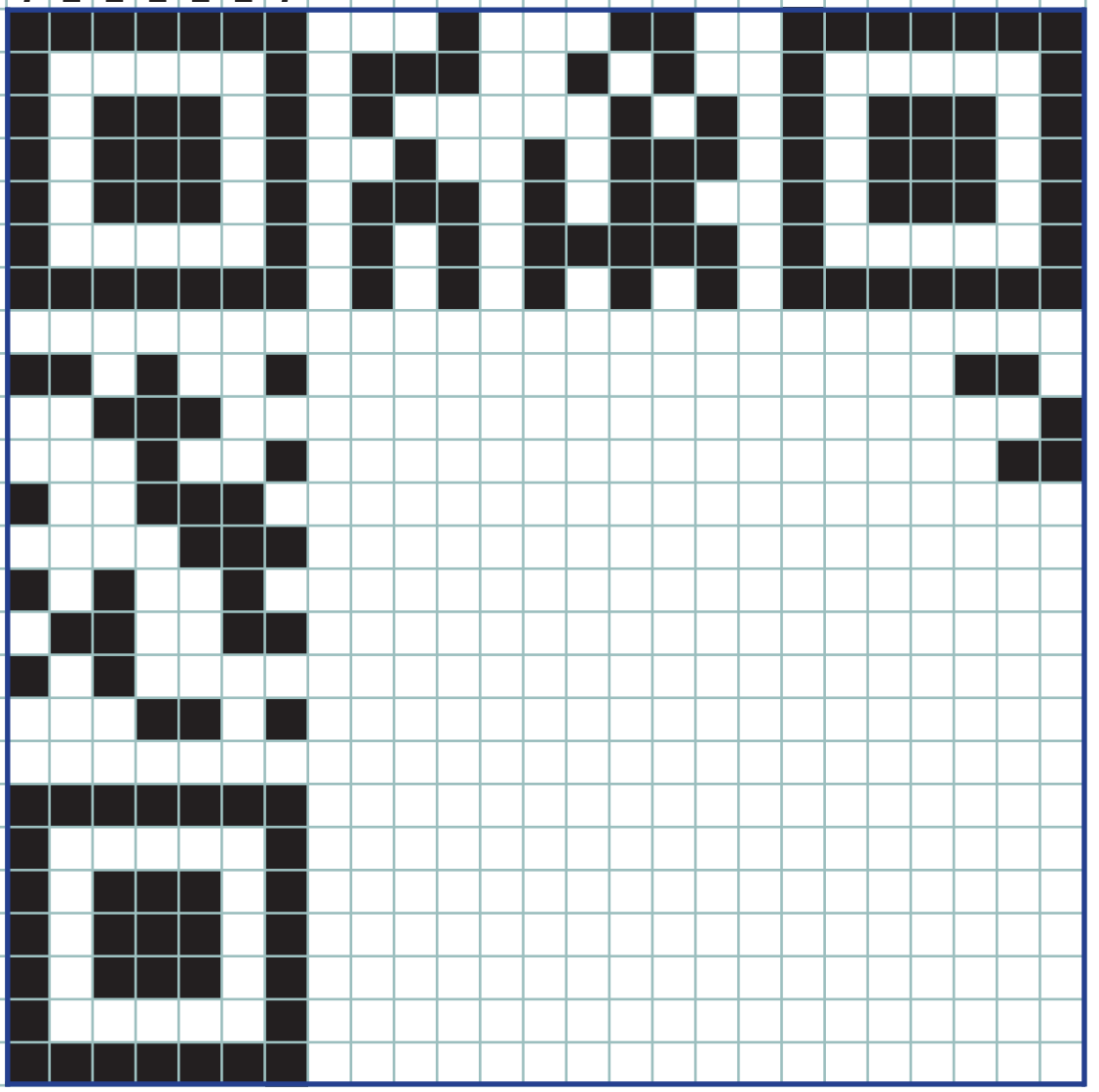
HEY! YOU SHOULD CHECK OUT JOFF'S TRAINING COURSE!

DEFINITELY!

THE ESCAPE ROOM CHALLENGE

	R							
C								
R1						7	1	2
R2			1	1	3	1	1	1
R3	1	3	1	1	1	1	1	3
R4	1	3	1	1	1	3	1	3
R5	1	3	1	3	1	2	1	3
R6			1	1	1	1	5	1
R7			7	1	1	1	1	1

	C1	C2	C3	C4	C5	C6	C7
					1		
			1	1	3		
			3	1	1		7
	7	1	1	1	1		1
	1	1	1	4	2	1	1
	1	1	3	1	1	1	1
	1	1	1	1	1	4	1
	1	1	3	3	3	1	1
	7	1	1	1	1	1	7



Embedded in these pages is a way to escape. A virtual escape room awaits, where you can experience your own chance to plant a shell and get out in time! In order to get there though, you'll need to scan the QR code on the next page. It seems like some of the data is still present, but most has been corrupted and needs to be reformed using picross. When you are sure you've recovered the QR code correctly, use a black marker on all filled-in spaces and leave the unused spaces blank, then scan away. If you've never heard of picross, that is okay! Go to this link to learn how to solve these puzzles: https://grandgamersguild.com/how-to-solve-picross-puzzle/

Good luck!

Download blank worksheets for the puzzle at:
https://www.blackhillsinfosec.com/prompt-zine

R. Real
I. Intelligence
T. Threat
A. Analytics

CHEAT SHEET

This poster is a quick reference guide to commonly used RITA commands and arguments. Additional RITA information and installation files can be found at: **https://github.com/activecm/rita**

CONFIGURATION

Command	Description
sudo nano /etc/rita/config.yaml	RITA configuration file.
rita test-config	Check the configuration file for validity.

INSTALLATION

Command	Description
sudo chmod +x ./install.sh	Make the install file executable.
sudo ./install.sh	Install RITA, as well as supported versions of Zeek and MongoDB.
sudo ./install.sh --disable-zeek --disable-mongo	Install RITA only, without Zeek or MongoDB. You can use these flags individually.

IMPORTING & ANALYZING DATA

Command	Description
mergecap -w *outfilename*.pcap *infilename1*.pcap *infilename2*.pcap	Merge multiple PCAP files into one PCAP file.
zeek -r *filename*.pcap local “Log::default_rotation_interval = 1 day”	Generate Zeek logs from a PCAP file.
rita import path/to/your/zeek_logs *datasetname*	One-off dataset import.
rita import --rolling /path/to/your/zeek_logs *datasetname*	Rolling datasets allow you to progressively analyze log data over a period of time.
/opt/zeek/logs/<date>	Default Zeek logs directory.

EXAMINING DATA

Command	Description
rita show-databases	Print the datasets currently stored.
rita show-beacons *datasetname*	Print hosts which show signs of C2 software.
rita show-beacons-fqdn *datasetname*	Print hosts which show signs of C2 software (FQDN Analysis).
rita show-strobes *datasetname*	Print strobe (fast beacon) information.
rita show-long-connections *datasetname*	Print long connections and relevant information.
rita show-useragents *datasetname*	Print user agent information.
rita show-exploded-dns *datasetname*	Print DNS analysis. Exposes covert DNS channels.
rita show-bl-hostnames *datasetname*	Print threat intel hostnames which received connections.
rita show-bl-source-ips *datasetname*	Print threat intel IPs which initiated connections.
rita show-bl-dest-ips *datasetname*	Print threat intel IPs which received connections.
rita html-report *datasetname*	Create an HTML report for an analyzed database.
rita delete-database *datasetname*	Delete imported database/dataset.

R.I.T.A. Real Intelligence Threat Analytics

Tool Shed

R14: 1 1 1 1 1 1 1 1 2 2 1

DONUT

https://github.com/TheWover/donut

R20: 1 1 1 1 1 1 5

Donut is a position-independent code that enables in-memory execution of VBScript, JScript, EXE, DLL files, and dotNET assemblies. A module created by Donut can either be staged from an HTTP server or embedded directly in the loader itself. The module is optionally encrypted using the Chaskey block cipher and a 128-bit randomly generated key. After the file is loaded and executed in memory, the original reference is erased to deter memory scanners.

PYPYKATZ

https://github.com/skelsec/pypykatz

Mimikatz implementation in pure Python. At least a part of it :) Runs on all OS's which support python>=3.6

version 0.4
by @itm4n

https://github.com/itm4n/PPLdump

This tool leverages a very clever trick that was initially discussed by James Forshaw in 2018. It involves the use of the DefineDosDevice API function to trick the system into creating an arbitrary Known DLL entry. Since PPLs do not check the digital signature of Known DLLs, this can be later used to perform a DLL hijacking attack and execute arbitrary code inside a PPL.

HELK

https://github.com/Cyb3rWard0g/HELK

The Hunting ELK, or simply the HELK, is one of the first open-source hunt platforms with advanced analytics capabilities such as SQL declarative language, graphing, structured streaming, and even machine learning via Jupyter notebooks and Apache Spark over an ELK stack.

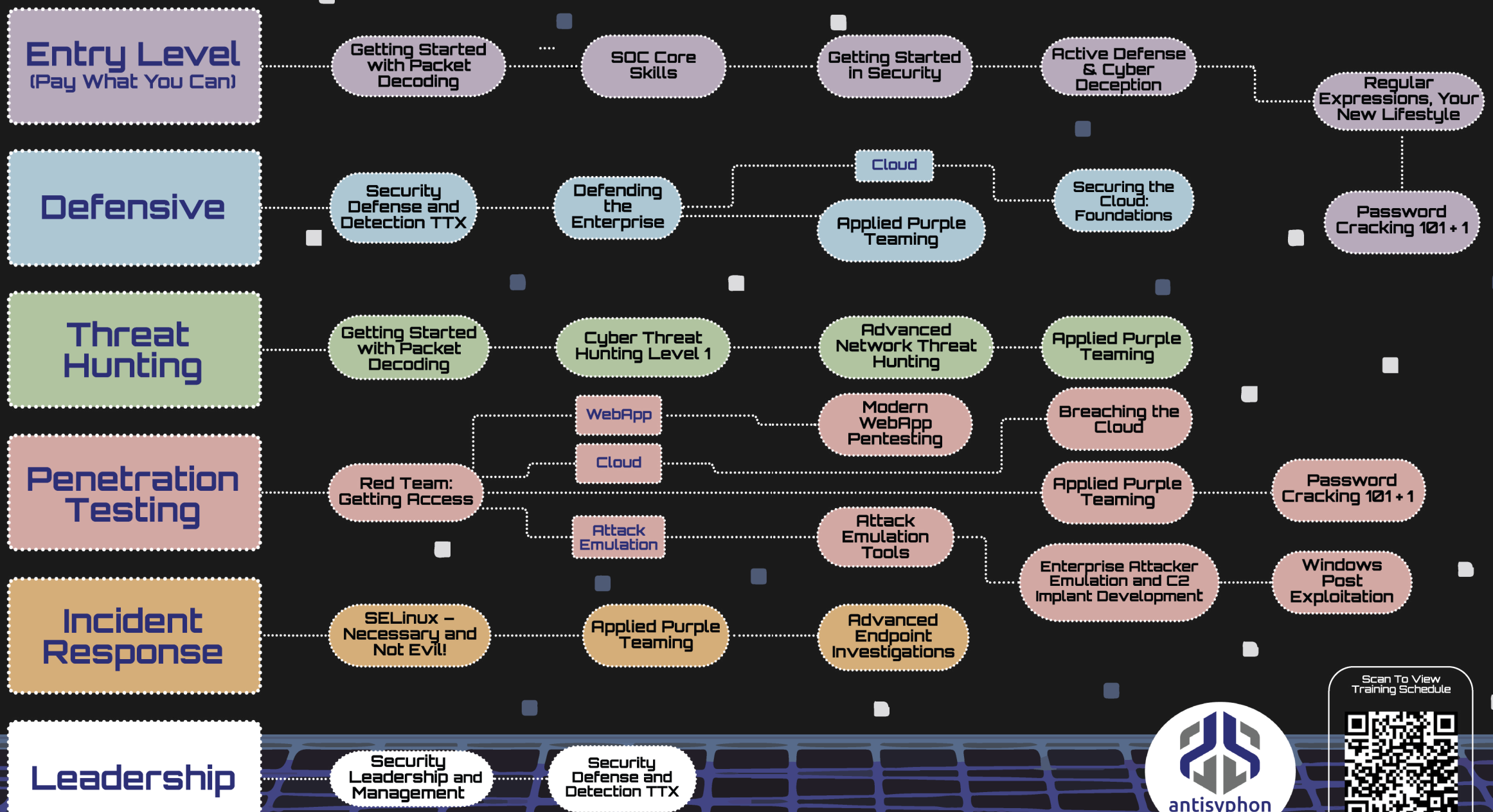
C13: 4 4 4 1

Training Trail

C17: 2 2 6 5 3

R17: 2 1 1 1 8

The Training Trail can help you figure out how various Antisyphon training courses offered through Wild West Hackin' Fest relate to one another. The far-left cell in each row contains the name of an infosec category (e.g., "Defensive"), and the cells to the right of that first cell in each row contain the names of training courses in that category (e.g., "Security Defense and Detection TTX"). You can use the Training Trail to find new courses to take and to help keep your infosec educational journey with Wild West Hackin' Fest on track.



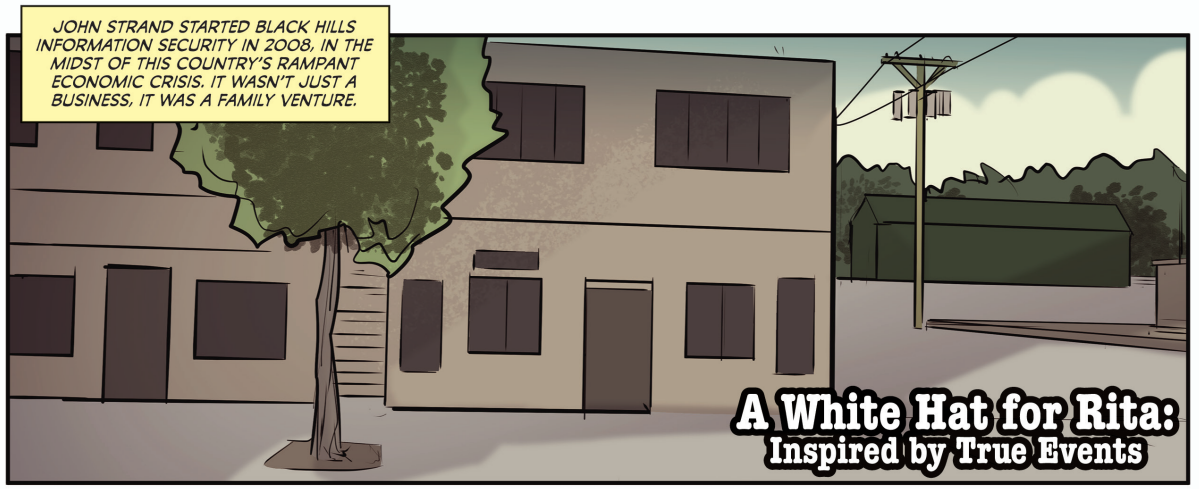
R19: 7 5 2 1 2 2

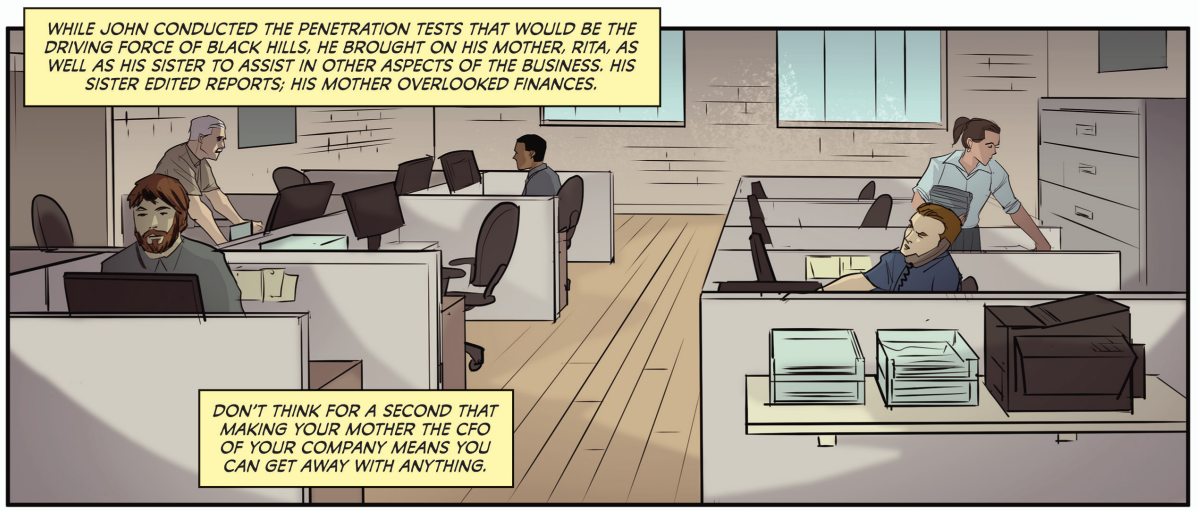
antisyphon
infosec training

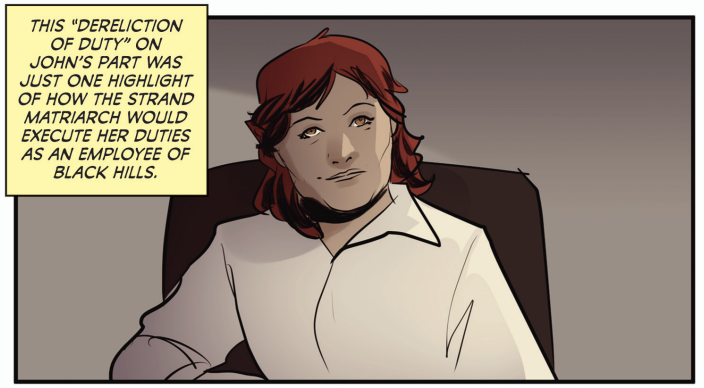
Scan To View Training Schedule

R12: 1 3 5 1 3

R13: 3 1 2 1 5 1 2







AN IMPORTANT PART OF PENETRATION TESTING IS WHAT COMES BEFORE IT: THE PASSIVE RECONNAISSANCE. WHEN A COMPANY WANTS TO TEST THEIR SYSTEM'S HACKABILITY, THE INITIAL QUESTION IS HOW TO GAIN ACCESS. GO THERE, IN PERSON, UNDETECTED, WITHOUT GIVING THE PLACE A CHANCE TO PREPARE OR PROTECT THEMSELVES.

ENTER RITA.

I WANT TO DO A PHYSICAL PEN TEST.

WHAT?

I WANNA BREAK INTO ONE OF THESE PLACES! I CAN DO IT!

MOM, SERIOUSLY? WHAT WE DO...IT BORDERS ON CRIMINAL, YOU HAVE TO COME UP WITH A RUSE--

JOHN, I'VE ALREADY GOT ONE.

YOU DO?

I'LL GO IN THERE FOR A FOOD SERVICE INSPECTION. THEY'LL LET ME RIGHT IN.

I WAS THE FOOD SERVICE DIRECTOR AT A HIGH SCHOOL. I KNOW ***EXACTLY*** WHAT TO SAY, WHAT TO SHOW THEM, AND WHERE TO GO. I'M ALSO NICE. THAT USUALLY WORKS TOO.

OKAY. LET'S FIND SOMEPLACE TO BREAK INTO.

JOHN HAD A FEW TARGETS IN MIND THAT PARTICULAR DAY, INCLUDING A PRISON.

DEFINITELY THE PRISON.

WHAT? NO, I'M NOT LETTING MY MOTHER BREAK INTO A PRISON!

ARE YOU KIDDING? I'LL BE IN AND OUT OF THERE, EASY PEASY!

RITA WOULD HAVE TO ESTABLISH CALLBACK DOCUMENTS AND GET A SHELL OUT OF THE PRISON. ONCE INSIDE, SHE'D BE TASKED WITH PLANTING USB DRIVES IN VARIOUS COMPUTERS. ALSO KNOWN AS RUBBER DUCKIES, THESE DRIVES CONTAINED AN EXECUTABLE FILE THAT WOULD DROP AN IMPLANT ONTO THE SYSTEM AS WELL AS A DOCUMENT EMBEDDED WITH A BEACON.

IF SOMEONE IS LOOKING OVER YOUR SHOULDER, OPEN THE DOCUMENT. IF THE COAST IS CLEAR, RUN THE EXECUTABLE FILE.

WHAT IS IT, LIKE A VIRUS?

NOT EXACTLY. IT'S A PROGRAM THAT WILL GIVE ME ACCESS TO THOSE COMPUTERS SO I CAN HACK INTO THEM FROM MY END.

SO IF SOMEONE WITH BAD INTENTIONS COULD HACK IN LIKE YOU, ***THEY*** COULD CONCEIVABLY GIVE THEM A VIRUS.

THAT'S WHAT WE'RE GONNA TRY TO STOP, YEAH.

WELL, THAT'S CERTAINLY NICE OF YOU.

WE CHOOSE TO WEAR THE WHITE HATS, MOM.

THAT'S GOOD. YOU'D LOOK LIKE AN UNDERTAKER IN A BLACK HAT.

THE DAY OF THE PEN TEST.

IT WAS TIME TO SEND RITA TO PRISON. ALONG WITH SOME COLLEAGUES, THE TEAM TRAVELED TO A COFFEE SHOP NEAR THE PRISON FOR THE PENETRATION TEST. EQUIPPED WITH SOME GLORIOUSLY LOW-TECH PROPS, RITA WAS READY TO GO.

JOHN, ON THE OTHER HAND, WAS HAVING SOME DOUBTS.

MOM, ARE YOU NERVOUS?

Shhhh, I'M GETTING INTO CHARACTER.

DINER

ONE LAST THING.

ASSUMING THEY DON'T TAKE YOUR PHONE, YOU'LL BE RECORDING THE WHOLE THING, SO WHEN YOU GET THE CHANCE, HERE'S HOW TO DO THAT...

SO, IF I GET ARRESTED, I'LL JUST SEND A RAVEN.

I CAN'T GUARANTEE IT WON'T HAPPEN.

JOHN, IT'LL BE FINE. IT'LL BE ***FUN.***

IN THE RENTAL CAR THEY ARRIVED IN, RITA DROVE OFF TO THE PRISON, LEAVING JOHN AND HIS COLLEAGUES BEHIND TO MONITOR RITA'S PROGRESS.

THERE SHE GOES.

I'M ASSUMING WE CAN FIND A CAR OR CAB OR SOMETHING IN CASE SOMETHING GOES AWRY?

DINER

I JUST SENT MY 58-YEAR-OLD MOTHER INTO A ***PRISON*** TO HACK INTO THEIR COMPUTERS.

THIS IS THE ***DUMBEST*** THING I HAVE EVER DONE.

I MEAN, WHAT'S THE WORST THAT COULD HAPPEN?

YOU OKAY?

NO!

ALL JOHN AND HIS TEAM COULD DO NOW WAS WAIT FOR THE SIGNAL FROM THE USB DRIVES THAT RITA WAS GOING TO PLANT. ASSUMING, OF COURSE, THAT SHE WOULD SUCCESSFULLY GET INSIDE THE PRISON.

TEN AGONIZING MINUTES--

--AND SEVERAL CUPS OF COFFEE--

--LATER...

TEN MORE AGONIZING MINUTES--

--AND SEVERAL MORE CUPS OF COFFEE--

--LATER...

TEN **MORE** AGONIZING MINUTES--

--AND SEVERAL **MORE** CUPS OF COFFEE--

--LATER...

WHAT IF SHE'S HANDCUFFED TO A DESK, BEING DENIED WATER...

DUDE...

A FEW MORE MINUTES LATER...

BLOOP

BLOOP

BLOOP

BLOOP

YOUR MOM'S *OKAY!*

NOT ONLY WAS RITA OKAY, SHE HAD CLEARLY ACCOMPLISHED HER MISSION.

BLOOP

BLOOP

BLOOP

AMONG THE NOTIFICATIONS WAS A SIGNAL INDICATING THAT ONE OF THE COMPUTER SYSTEMS THAT CALLED BACK BELONGED TO THE DIRECTOR OF THE PRISON.

SHE DID IT.

YOUR MOM...

SHE *DID* IT.

LATER...

SO, HOW'D I DO?

OPEN

DO I GET A WHITE HAT?

MOM, YOU ARE OFFICIALLY A WHITE HAT HACKER. OR AT LEAST AN HONORARY ONE.

SUPER. BY THE WAY, DO YOU REMEMBER SAM OWENS? YOU WENT TO HIGH SCHOOL WITH HER. SHE WORKS THERE!

SHE'S DOING GREAT! SHE HAS THREE KIDS--

MOM, THIS IS NOT THE STORY I WANT TO HEAR ABOUT RIGHT NOW.

OH! RIGHT. WELL, LIKE I SAID, IT WAS EASY!

"I WALKED RIGHT UP TO THE FRONT, SAID I WAS WITH THE HEALTH DEPARTMENT, AND THAT THIS WAS A SURPRISE INSPECTION. AFTER THAT, THEY PRACTICALLY GAVE ME THE RUN OF THE PLACE, ASKED ME WHERE I NEEDED TO GO. SO I SAID, "TAKE ME TO ALL OF YOUR COMPUTERS." JUST KIDDING. ACTUALLY, NOT REALLY. I HAD THEM BRING ME TO THE NEWC."

"THE NEWC?"

"THE NETWORK OPERATION CENTER. MAYBE IT'S NOC? THEY KNEW WHAT I MEANT.

"ANYWAY, THEY TOOK ME RIGHT THERE, ALONG WITH YOUR STANDARD FOOD PREPARATION AND SERVICE LOCATIONS, LET ME WALK AROUND ***BY MYSELF.*** I FIGURED WHILE I WAS THERE I'D DO A FULL INSPECTION SINCE I HAD MY LASER THERMOMETER HANDY."

"DID YOU FIND ANYTHING?"

"THEIR FRIDGE WAS TOO WARM. I HOPE THEY DON'T HAVE TOO MUCH DAIRY ON THEIR MENU. ANYWAY, I STUCK THE DRIVES IN ALL THE COMPUTERS I COULD FIND, CLICKETY-CLACK, RELEASED THE HOUNDS, AND WENT BACK TO THE FRONT DESK TO INFORM THEM ABOUT THEIR BUSTED REFRIGERATOR. AND SOME MOLD."

"AND THAT WAS THAT?"

"*Ehhh,* NOT QUITE."

I WAS TOLD THE DIRECTOR WANTED TO SEE ME, WHICH MADE ME WONDER IF I'D BEEN ***MADE.*** WHEN I GOT TO HIS OFFICE, HE WANTED TO KNOW WHAT THEIR SCORE WAS ON THE ***FOOD INSPECTION,*** AND IF THERE WAS ANYTHING THEY COULD DO TO PREPARE FOR ANOTHER ONE.

NOW, I FIGURED THE DIRECTOR WAS A PRETTY BIG FISH, SO I GAVE HIM A DRIVE AND SAID THERE WAS A SELF-CHECKLIST ON IT THAT HE COULD FILL OUT.

AND THEN WE GOT THE CONNECTION.

AND NOW HE KNOWS HE HAS MOLD.

I'D REALLY LIKE A WIDE BRIM, SOMETHING THAT WILL PROTECT MY COMPLEXION FROM THE SUN BUT LOOKS GOOD WITH OUTFITS.

SO, WHAT WAS THEIR SCORE?

FOR A PLACE THAT'S SUPPOSED TO BE PRETTY LOCKED DOWN, I THINK THEY DID PRETTY LOUSY. I MEAN, NO ONE EVEN CALLED TO SEE IF I WAS REALLY FROM THE HEALTH DEPARTMENT, AND THEY JUST LET ME WALTZ INTO THEIR COMPUTER ROOM UNSUPERVISED! BUT NOW YOU CAN HELP THEM, RIGHT?

WE SURE CAN TRY.

I SURE HOPE SO. BECAUSE THE GUYS ON THE OTHER SIDE OF THOSE BARS...IT SHOULDN'T BE AS EASY FOR THEM TO BREAK OUT AS IT WAS FOR US TO BREAK IN.

I FELT LIKE A SECRET AGENT.

YOU KINDA WERE ONE! AND YOU DID GREAT. I COULDN'T BE MORE PROUD.

IT'S A FUNNY THING, DOING THIS IN A PRISON.

WHY IS THAT?

WELL, WHAT YOU DO... YOU COULD EITHER END UP BEHIND BARS OR BE THE GUY WHO HELPS STOP THE ONES WHO SHOULD BE. BUT YOU CHOSE WISELY.

WHAT CAN I SAY? YOU TAUGHT ME WELL.

RITA'S FIRST SUCCESSFUL PENETRATION TEST ENDED UP BEING HER ONLY ONE. A FEW MONTHS AFTER HER TRIP TO PRISON, SHE WAS DIAGNOSED WITH PANCREATIC CANCER AND DIED LESS THAN A YEAR LATER. SHE DIDN'T LEAVE THIS EARTH WITHOUT A FIGHT, AND NOT LONG BEFORE SHE PASSED AWAY, SHE TOLD JOHN THAT SHE ALWAYS KNEW HE'D GROW UP TO BE EITHER A CRIMINAL OR SUPERMAN.

SHE WAS RIGHT. HE CHOSE WISELY.

JOHN STRAND, AGE 4

THE END

ORIGINAL STORY: John Strand

WRITER/EDITOR: Jamie Frevele (@jamiefrevele on Twitter) **ARTIST: Joe Eisma** (@supajoe)

COLORIST: Shari Chankhamma (@sharihes on Twitter) **LETTERER: Taylor Esposito** (@taylorespo on Twitter)

PROMPT#

Coloring Contest

Details: https://www.blackhillsinfosec.com/prompt-zine/

"The bears in the woods that are chasing you have rocket packs, AK-47s, flamethrowers, and they kill indiscriminately."