
PROMPT#
SPECIAL EDITION
COMIC BOOK ADAPTATION
Presents:
DARKNET DIARIES
EPISODE 36: JEREMY IN MARKETING

These are true stories from the dark side of the internet.

Big thanks to Jack Rhysider for letting us turn an episode of Darknet Diaries into a comic book. Jack is an amazing storyteller who has really brought attention to the important work we do in information security.

And shoutout to Tinker Secor for sharing his story as a penetration tester in a way that teaches us all something valuable.

Original Story: **Tinker Secor**
Darknet Diaries Episode: **Jack Rhysider**

Listen to the inspiration here:
https://darknetdiaries.com/episode/36/

Comic Book Adaptation

Writer: **John Arcudi**
Interior Artist/Colorist: **Owen Gieni**
Letterer: **Taylor Esposito**
Cover Artist: **odibagas**
Editor: **Joseph Keatinge**
Copy Editor: **Deb Wigley**

PROMPT# is a Black Hills Information Security project.
This comic book was produced in association with REKCAH Publishing.
Chief Creative Officers: **Jason Blanchard & John Strand**

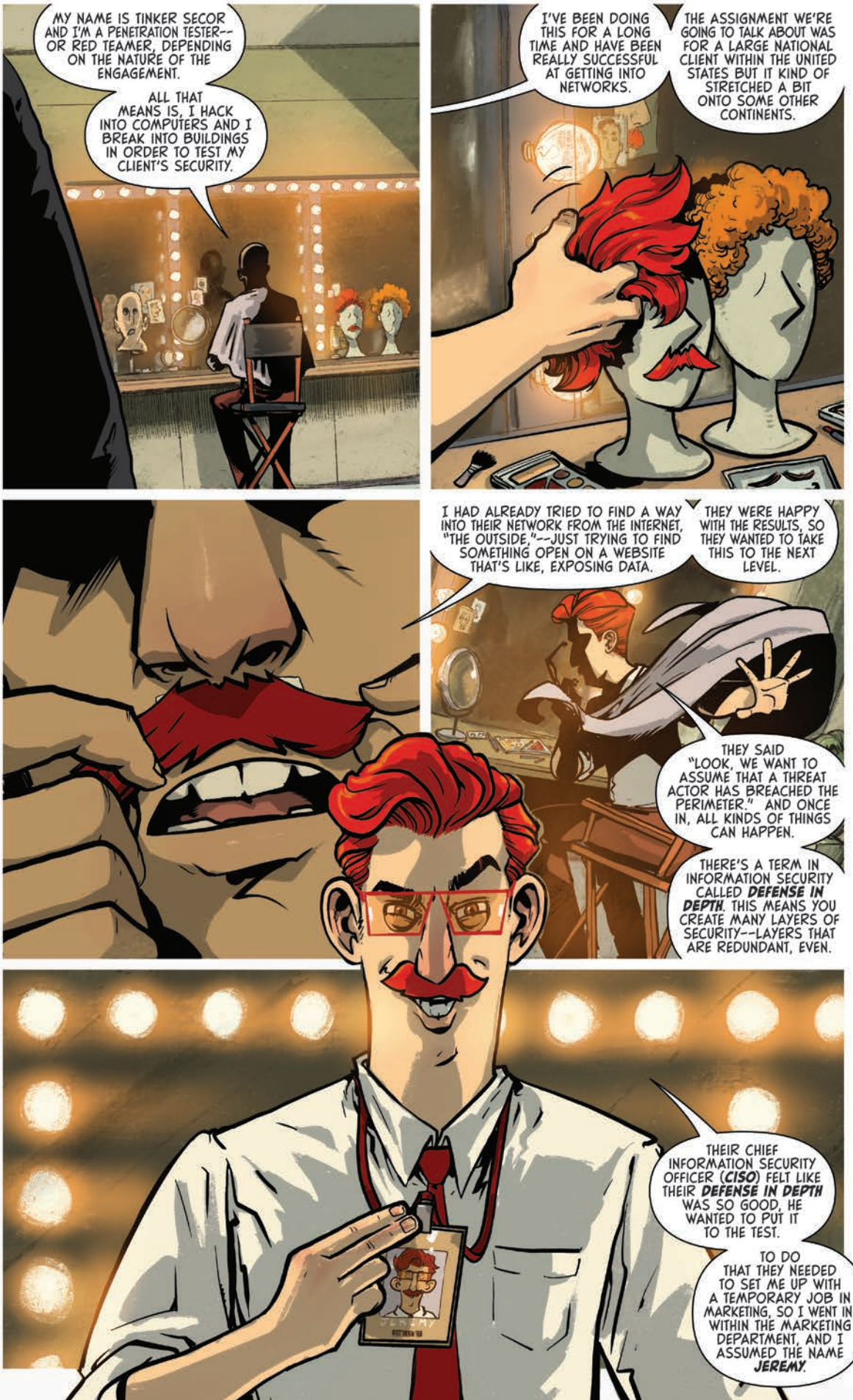
Black Hills Information Security
PROMPT#
Mailing address:
PO Box 970, Spearfish, SD 57783
Subscribe to get future issues of PROMPT#

www.promptzine.com


HI, I'M JACK, THE HOST OF THIS COMIC AND OF THE *DARKNET DIARIES* PODCAST.
BUT MY LAST JOB WAS LOOKING AT MY CLIENT'S NETWORKS TO TRY TO FIND WAYS TO MAKE THEM MORE SECURE. IN OTHER WORDS, I WAS ON DEFENSE, LOCKING THINGS DOWN, HARDENING SYSTEMS, SECURING APPLICATIONS AND THE LIKE. THE DEFENSE TEAM IS SOMETIMES KNOWN AS THE ***BLUE TEAM.***
BUT ONE DAY WE PAID A PROFESSIONAL ***"PENETRATION TESTER"*** TO COME INTO OUR OFFICE AND SEE HOW WELL I DID AT SECURING THE NETWORK. ATTACKERS LIKE THIS ARE SAID TO BE ON THE ***RED TEAM*** AND THIS WHOLE RED TEAM/BLUE TEAM THING IS JUST A TERM BORROWED FROM THE MILITARY WHERE THEY HAVE DRILLS WITH ATTACKERS AND DEFENDERS.
NOW, IMAGINE IF A BRICK AND MORTAR-TYPE STORE TESTED THEIR SECURITY LIKE THIS TOO. YOU'D HAVE PAID SHOPLIFTERS TRYING TO TEST HOW GOOD THEIR SECURITY IS. YOU'D PAY CAT BURGLARS TO TRY TO STEAL PAINTINGS FROM MUSEUMS AND YOU'D HAVE REFORMED STREET GANGSTERS TRYING TO QUIETLY ROB A CASINO. MAYBE SOME OF THESE JOBS EXIST BUT IN THE ONLINE WORLD IT'S ACTUALLY VERY COMMON.


ANYWAY, WITH ***MY*** "PEN TESTER," I WATCHED OVER HIS SHOULDER FOR THE WHOLE WEEK HE WAS THERE AND I WAS AMAZED AT WHAT HE COULD DO!
IT MADE A PERMANENT IMPACT ON THE WAY I SEE HOW ATTACKERS WORK.
PROP BOX


I WANT TO GIVE YOU THAT EXPERIENCE SO I'M GOING TO INTRODUCE YOU TO A PENETRATION TESTER TO SEE EXACTLY HOW HE DOES HIS JOB--WHICH IS TRYING TO BREAK THROUGH A COMPANY'S SECURITY SYSTEMS AND GET THE "CROWN JEWELS."


MY NAME IS TINKER SECOR AND I'M A PENETRATION TESTER--OR RED TEAMER, DEPENDING ON THE NATURE OF THE ENGAGEMENT.
ALL THAT MEANS IS, I HACK INTO COMPUTERS AND I BREAK INTO BUILDINGS IN ORDER TO TEST MY CLIENT'S SECURITY.
I'VE BEEN DOING THIS FOR A LONG TIME AND HAVE BEEN REALLY SUCCESSFUL AT GETTING INTO NETWORKS.
THE ASSIGNMENT WE'RE GOING TO TALK ABOUT WAS FOR A LARGE NATIONAL CLIENT WITHIN THE UNITED STATES BUT IT KIND OF STRETCHED A BIT ONTO SOME OTHER CONTINENTS.
I HAD ALREADY TRIED TO FIND A WAY INTO THEIR NETWORK FROM THE INTERNET, "THE OUTSIDE,"--JUST TRYING TO FIND SOMETHING OPEN ON A WEBSITE THAT'S LIKE, EXPOSING DATA.
THEY WERE HAPPY WITH THE RESULTS, SO THEY WANTED TO TAKE THIS TO THE NEXT LEVEL.
THEY SAID "LOOK, WE WANT TO ASSUME THAT A THREAT ACTOR HAS BREACHED THE PERIMETER." AND ONCE IN, ALL KINDS OF THINGS CAN HAPPEN.
THERE'S A TERM IN INFORMATION SECURITY CALLED DEFENSE IN DEPTH. THIS MEANS YOU CREATE MANY LAYERS OF SECURITY--LAYERS THAT ARE REDUNDANT, EVEN.
THEIR CHIEF INFORMATION SECURITY OFFICER (CISO) FELT LIKE THEIR DEFENSE IN DEPTH WAS SO GOOD, HE WANTED TO PUT IT TO THE TEST.
TO DO THAT THEY NEEDED TO SET ME UP WITH A TEMPORARY JOB IN MARKETING, SO I WENT IN, WITHIN THE MARKETING DEPARTMENT, AND I ASSUMED THE NAME JEREMY.


THERE'S REALLY ONLY TWO PEOPLE IN THE ENTIRE COMPANY WHO KNEW WHO I WAS: THE CISO AND ONE OF HIS ASSISTANTS.
THEY SAID I COULD BRING IN ANYTHING I WANTED. I COULD BRING IN ALL MY HACKING GEAR IF I WANTED TO BUT I NEEDED TO MAKE SURE THAT I DIDN'T GET CAUGHT.
"I HAD IN MY BACKPACK MY OWN HACK BOX, JUST A LITTLE DELL LAPTOP LOADED WITH UBUNTU AS A BASE IMAGE WITH SOME KALI VMS, ETC.
"BUT I WASN'T GOING TO BRING IN EXTRA LAPTOPS OR HAVE A BUNCH OF ANTENNAE STICKING OUT OF MY DESK DRAWERS. TOO SUSPICIOUS."
"THE TEAM WAS TOLD THAT I WAS A CONTRACTOR. THIS COMPANY USED A DECENT AMOUNT OF CONTRACTORS SO MY BEING THERE WAS FAIRLY NORMAL AND WOULDN'T ATTRACT ANY ATTENTION.
HERE'S YOUR CUBICLE! HERE'S YOUR TEAM.
"STILL, I NEEDED TO KEEP IT THAT WAY. MY AIM AT THE BEGINNING IS JUST SIT VERY, VERY STILL AND LISTEN TO WHAT'S GOING ON AROUND ME, GET A FEEL FOR THE ENVIRONMENT.
"AS THE SPIRITUAL TEACHER RAM DASS SAID, 'THE QUIETER YOU BECOME THE MORE YOU CAN HEAR.'"

"NOT A LOT WAS EXPECTED OF ME WITHIN THE FIRST COUPLE WEEKS IN THE MARKETING DEPARTMENT. IT WAS LIKE, "JUST WATCH THE SECURITY VIDEOS, DON'T CLICK ON A PHISH EMAIL" THAT SORT OF THING. SO, I'M LEFT ALONE, SEE?

"THE VERY FIRST THING I CAN DO IS PULL UP ***CMD.EXE*** ON THE WORKSTATION. I'M USING ***THEIR*** TOOLS. I'M NOT USING MALWARE!

"I JUST TYPE IN ***NET USERS /DOMAIN*** AND IT WILL DUMP OUT THE ENTIRE LIST OF ALL USERS WITHIN THAT DOMAIN. I CAN DO ***NET GROUPS "DOMAIN ADMINS" /DOMAIN*** AND DUMP ALL THE DOMAIN ADMINS.

"I CAN DO ***NET GROUPS "DOMAIN CONTROLLERS" /DOMAIN*** AND DUMP OUT THE HOST NAMES OF ALL THE DOMAIN CONTROLLERS. IT'S A TON OF DATA.

"RUNNING THESE COMMANDS AS A USER AGAINST THE DOMAIN CONTROLLER IS HOW A LOT OF DEFAULT ACTIVE DIRECTORY ENVIRONMENTS ARE SET UP.

"***ACTIVE DIRECTORY*** IS THE MECHANISM THAT WINDOWS COMPUTERS AUTHENTICATE TO EACH OTHER. IT HAS INFORMATION ON ALL THE USERS AND ALL THE PASSWORDS AND IT HAS TONS OF STUFF THAT HACKERS CAN USE TO ESCALATE THEIR PRIVILEGES OR MOVE ON TO OTHER SYSTEMS.

"SO "JEREMY FROM MARKETING" PULLS OUT MY ROGUE LAPTOP AND BOOTS IT UP. NOW I'M GOING TO RUN ***WIRESHARK.***

"PRIMARILY WHAT I WAS LOOKING FOR WAS WHAT SORT OF HARDWARE IS ON THE NETWORK; LAPTOP-WISE OR EVEN SERVER WISE. WHAT'S THE HOST'S NAME SCHEMA?

"WHILE ***WIRESHARK*** GENERALLY ONLY PICKS UP TRAFFIC TO YOUR COMPUTER, IT ALSO PICKS UP BROADCAST TRAFFIC, TOO. THESE ARE PACKETS THAT ARE INTENDED FOR EVERYONE ON THAT SUBNET AND COMPUTERS MAKE A LOT OF BROADCAST TRAFFIC.

"CAPTURING THESE MAC ADDRESSES, IT WILL ALSO TELL YOU WHAT KIND OF SYSTEMS ARE ON THE NETWORK BECAUSE A MAC ADDRESS CONTAINS INFORMATION ON WHAT MANUFACTURER MADE THAT DEVICE.

"AS I FOUND THESE LAPTOPS AND SERVERS, I LEARNED THE HOST NAMES AND I CHANGED MY HOST NAME TO MATCH THEIR SCHEMA AND CHANGED MY MAC ADDRESS TO MATCH THEIR HARDWARE.

"THINK OF IT AS RAMBO PAINTING HIMSELF WITH MUD TO AVOID DETECTION."

"DAY ONE WAS OVER, AND I GOTTA TELL YA', I WAS FEELING PRETTY CONFIDENT.

"I COLLECTED A LOT OF DATA AND HAD A FEEL FOR THE ENVIRONMENT. I WAS CONFIDENT THAT I COULD START DOING MORE ACTIVE RECONNAISSANCE WITHOUT BEING FOUND OUT.

"DAY TWO, AND I DECIDED THAT IT WAS TIME TO FIRE UP RESPONDER.

Back space

Enter

KLIK

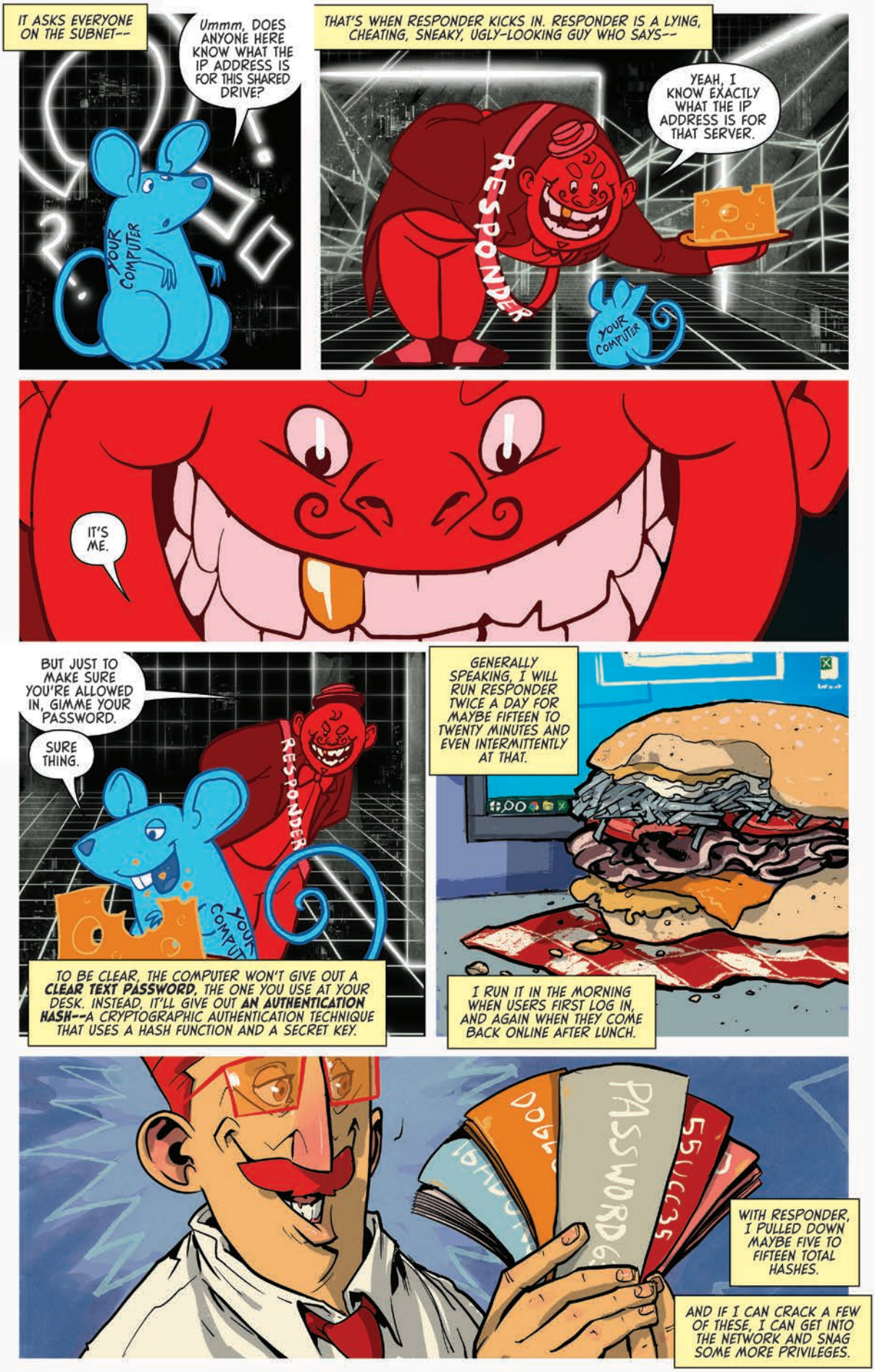
"IN MY OPINION RESPONDER IS AN AMAZING TOOL. Y'SEE, MANY OFFICES HAVE SHARED DRIVES SO THAT MORE PEOPLE CAN ACCESS CERTAIN FILES. NOW, SUPPOSE YOUR WINDOWS COMPUTER NEEDS TO CONNECT TO THIS SHARED NETWORK DRIVE.

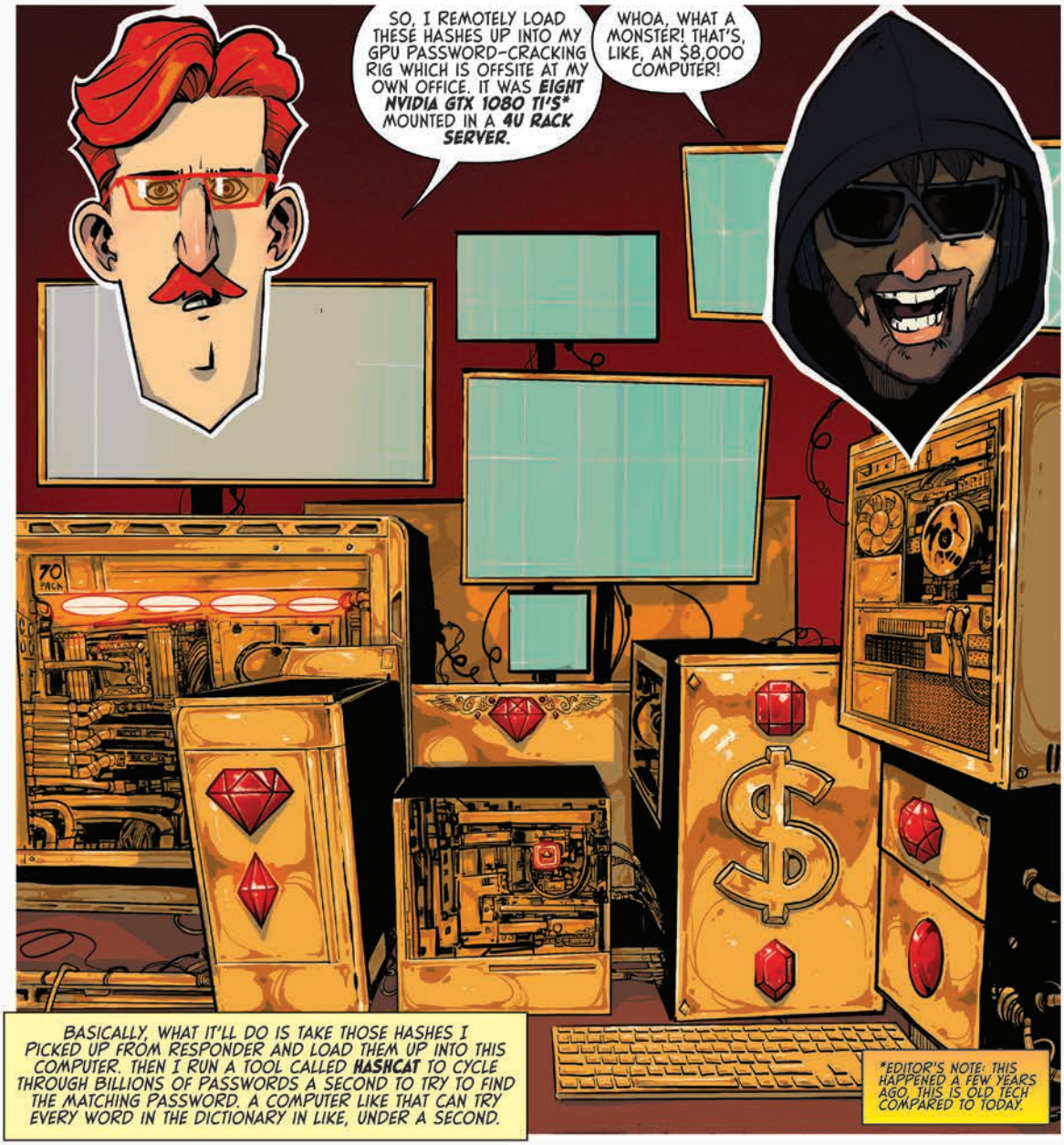
"IT WILL TRY A FEW THINGS, BUT IF THOSE DON'T WORK, IT'LL GO TO THE OFFICE'S DOMAIN NAME SYSTEM ***(DNS)*** TO SEE IF IT KNOWS THE IP ADDRESS FOR THE SHARED DRIVE.

"AN IP ADDRESS IS LIKE A PHONE NUMBER FOR COMPUTERS TO CONTACT EACH OTHER."

YOUR COMPUTER

"USUALLY, THAT WORKS, BUT OCCASSIONALLY--FOR A VARIETY OF REASONS--IT FAILS AND THAT'S WHEN YOUR COMPUTER GETS DESPERATE."


IT ASKS EVERYONE ON THE SUBNET--
Ummm, DOES ANYONE HERE KNOW WHAT THE IP ADDRESS IS FOR THIS SHARED DRIVE?
YOUR COMPUTER
THAT'S WHEN RESPONDER KICKS IN. RESPONDER IS A LYING, CHEATING, SNEAKY, UGLY-LOOKING GUY WHO SAYS--
YEAH, I KNOW EXACTLY WHAT THE IP ADDRESS IS FOR THAT SERVER.
RESPONDER
YOUR COMPUTER
IT'S ME.
BUT JUST TO MAKE SURE YOU'RE ALLOWED IN, GIMME YOUR PASSWORD.
SURE THING.
RESPONDER
YOUR COMPUT
TO BE CLEAR, THE COMPUTER WON'T GIVE OUT A CLEAR TEXT PASSWORD, THE ONE YOU USE AT YOUR DESK. INSTEAD, IT'LL GIVE OUT AN AUTHENTICATION HASH--A CRYPTOGRAPHIC AUTHENTICATION TECHNIQUE THAT USES A HASH FUNCTION AND A SECRET KEY.
GENERALLY SPEAKING, I WILL RUN RESPONDER TWICE A DAY FOR MAYBE FIFTEEN TO TWENTY MINUTES AND EVEN INTERMITTENTLY AT THAT.
I RUN IT IN THE MORNING WHEN USERS FIRST LOG IN, AND AGAIN WHEN THEY COME BACK ONLINE AFTER LUNCH.
PASSWORD
WITH RESPONDER, I PULLED DOWN MAYBE FIVE TO FIFTEEN TOTAL HASHES.
AND IF I CAN CRACK A FEW OF THESE, I CAN GET INTO THE NETWORK AND SNAG SOME MORE PRIVILEGES.


SO, I REMOTELY LOAD THESE HASHES UP INTO MY GPU PASSWORD-CRACKING RIG WHICH IS OFFSITE AT MY OWN OFFICE. IT WAS **EIGHT NVIDIA GTX 1080 TI'S*** MOUNTED IN A **4U RACK SERVER.**
WHOA, WHAT A MONSTER! THAT'S, LIKE, AN $8,000 COMPUTER!
BASICALLY, WHAT IT'LL DO IS TAKE THOSE HASHES I PICKED UP FROM RESPONDER AND LOAD THEM UP INTO THIS COMPUTER. THEN I RUN A TOOL CALLED **HASHCAT** TO CYCLE THROUGH BILLIONS OF PASSWORDS A SECOND TO TRY TO FIND THE MATCHING PASSWORD. A COMPUTER LIKE THAT CAN TRY EVERY WORD IN THE DICTIONARY IN LIKE, UNDER A SECOND.
*EDITOR'S NOTE: THIS HAPPENED A FEW YEARS AGO. THIS IS OLD TECH COMPARED TO TODAY.


THEN IT'LL TRY ADDING NUMBERS TO THE ENDS OF WORDS, OR SPECIAL SYMBOLS LIKE A DOLLAR SIGN INSTEAD OF AN "S." IT WILL KEEP TRYING PASSWORDS MORE RANDOM AND MORE COMPLEX OVER TIME UNTIL IT FINDS A MATCH. IT'S RULE-BASED HASH-CRACKING.
IT WAS RUNNNING BETWEEN, I DON'T KNOW, SIX TO TWELVE BILLION GUESSES PER SECOND. THE LOWEST I'VE EVER GOTTEN FROM THIS RIG WAS LIKE, A 20% CRACK RATE.
CRACK!


BUT I DIDN'T CRACK **ANY!**

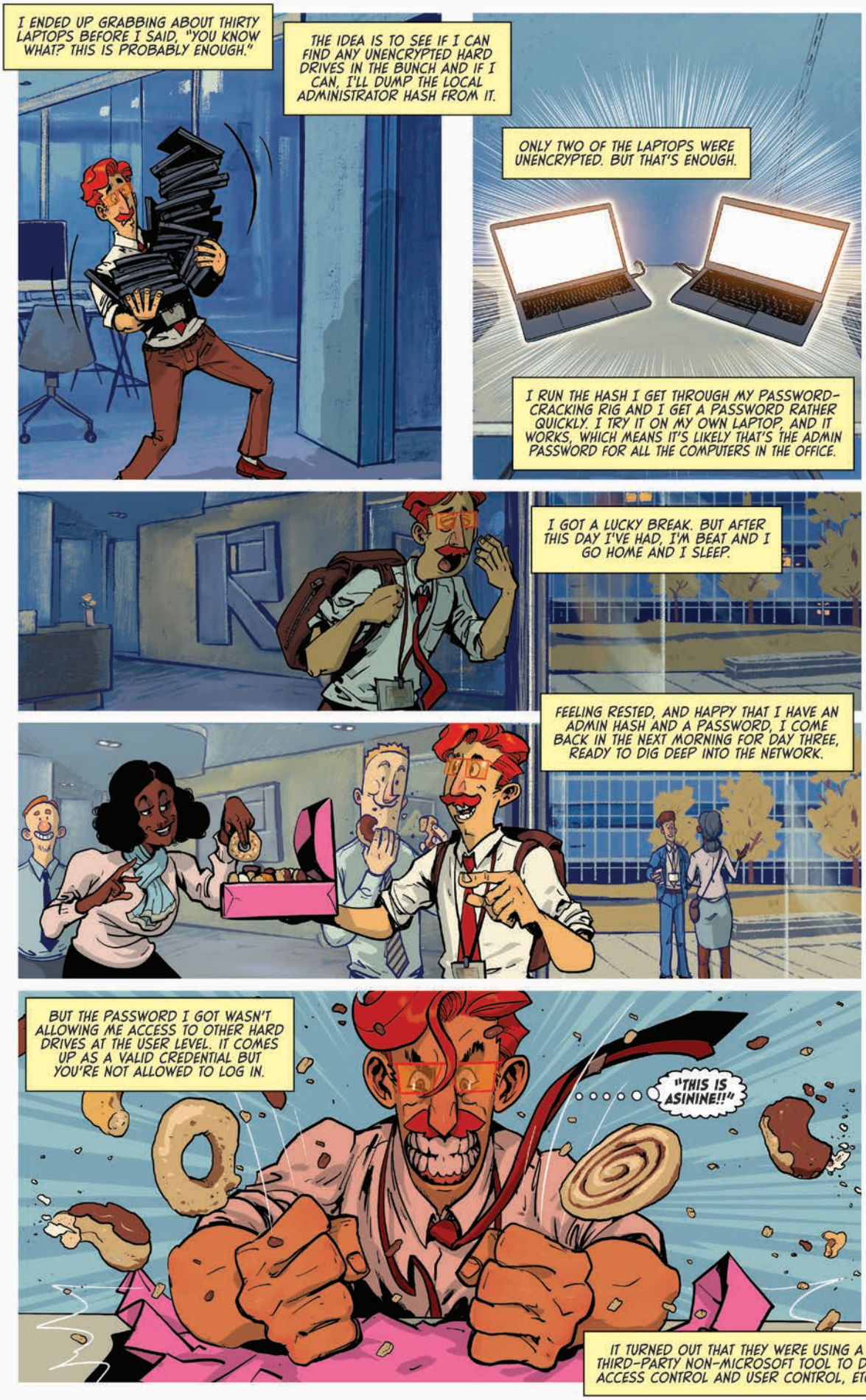

USUALLY WHEN THAT HAPPENS IT MEANS MY TOOLS ARE BROKEN, LIKE BY AN UPDATE OR SOMETHING. BUT I RAN TESTS ON THEM AND THEY WERE ALL FINE.
NEXT I CHECKED THE SECURITY POLICY, AND SURE ENOUGH, THEY HAD A MINIMUM OF TWELVE CHARACTERS REQUIRED FOR PASSWORDS -- OR WHAT END UP BEING "PASSPHRASES."
CLACK
CLICK
TAC TAC
TAP TAP TAP
CLACKETY
TAPETY
I'M A BIG ADVOCATE OF PASSPHRASES.
PASSWORDS, YOU CAN CRACK FAIRLY EASILY, BUT A PASSPHRASE, IDEALLY FOUR OR FIVE DIFFERENT WORDS, COMPLETELY RANDOM, THAT'S MUCH MORE ROBUST, MUCH MORE DIFFICULT TO CRACK.
BUT NOT IMPOSSIBLE!
I CHANGED SOME OF MY ATTACK SETTINGS TO ACCOUNT FOR MINIMUM TWELVE CHARACTERS, AND BASICALLY JUST PICKED LONGER WORDS AND LONGER NUMBERS AT THE END.
I DID THAT, AND I GOT A COUPLE OF CLEAR TEXT PASSWORDS.
STILL, LET ME TELL YOU, MY EQUIPMENT WAS SWEATING AFTER THAT!

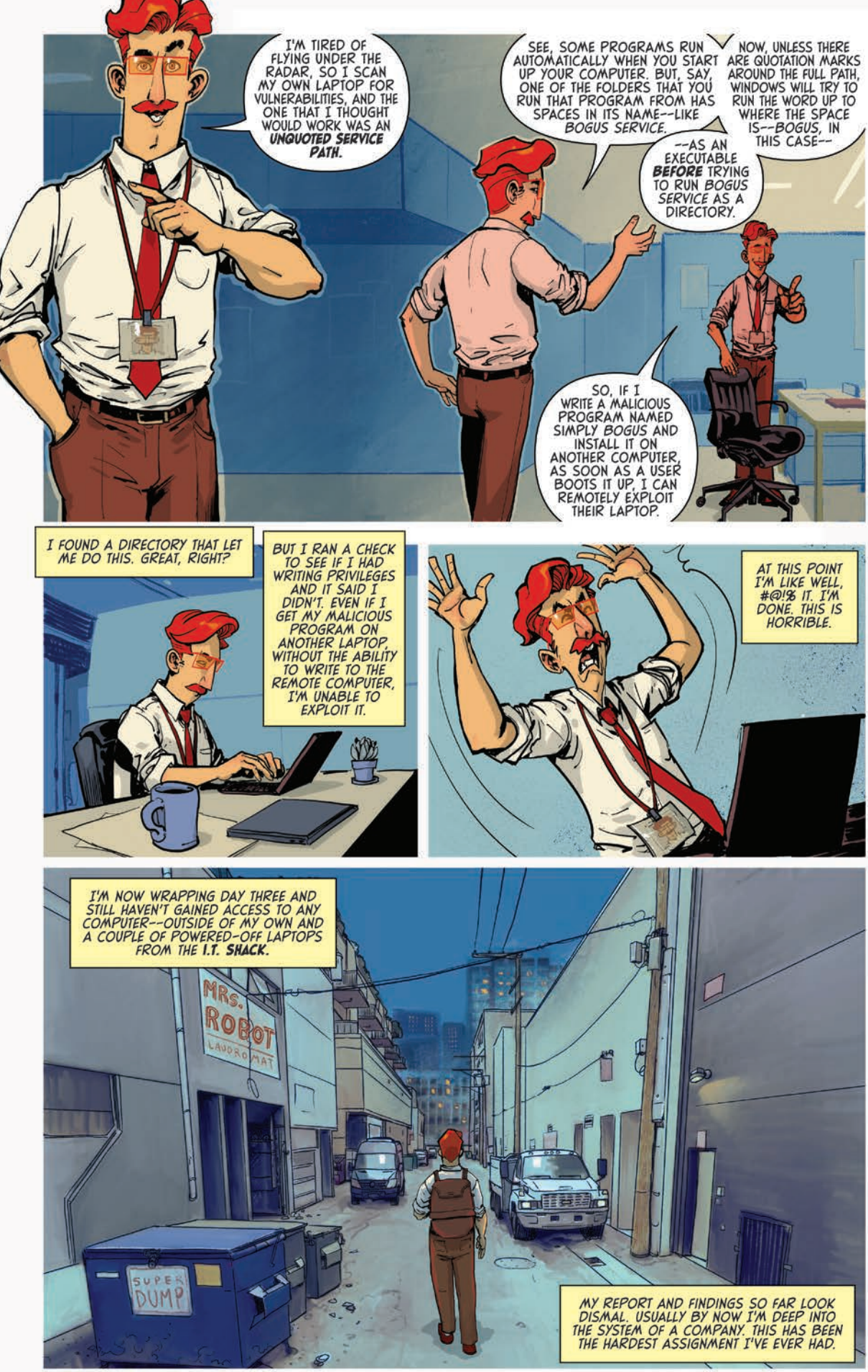

SO, I LOG OUT OF MY LAPTOP AS MYSELF AND THEN LOG BACK IN USING ONE OF THESE STOLEN CREDENTIALS.
I DON'T WANT ANY OF THIS TIED BACK TO ME AS A PERSON.
I START SEARCHING THROUGH THE EMAILS OF THIS OTHER PERSON BUT ALL I FIND IS A PASSWORD FOR A THIRD-PARTY WEBSITE--**NOTHING** INSIDE THE COMPANY.
SO, I TRIED A DIFFERENT APPROACH. GET INTO THEIR **SINGLE SIGN-ON.** SINGLE SIGN-ON IS A SINGLE PORTAL FOR EMPLOYEES TO LOG INTO WHICH THEN PROVIDES THEM ACCESS TO ALL THE TOOLS THEY NEED, AND IT'S A HACKER'S DREAM!
I'VE TAKEN DOWN ENTIRE ORGANIZATIONS WHERE SINGLE SIGN-ON WAS THERE, LIKE A HUB OF APPLICATIONS, IF YOU WILL. ONE STOP HACKING!
WITH THESE STOLEN CREDENTIALS, I WAS ABLE TO LOG INTO THEIR PORTAL AND THERE I FOUND A BUNCH OF DIFFERENT APPS, PAYROLL STUFF, CLIENT DATABASES, CONTROL PANELS.
DATABASES
CONTROL PANELS
PAYROLL
APPLICATIONS
DATA
PAYROLL
APPS
CLIENT
PANELS
BUT WHEN I CLICKED ON ONE OF THE APPS...
Multi-factor authentication
Authentication code
Verify
EACH INDIVIDUAL APP REQUIRED ITS OWN SEPARATE MULTI-FACTOR AUTHENTICATION LOGIN.
I WAS LIKE, WHAT KIND OF LOCKDOWN PRISON IS THIS PLACE?

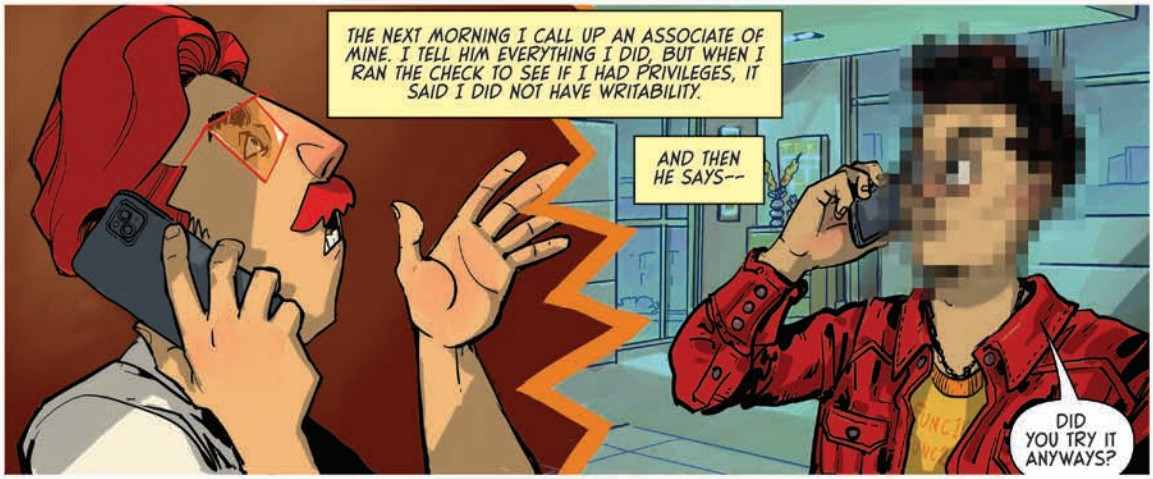

ONE THING THAT CAUGHT MY EYE THOUGH, IN THE SINGLE SIGN-ON, WAS **CITRIX.**
WHAT CITRIX AMOUNTS TO IS A REMOTE DESKTOP THROUGH THE BROWSER. USING THAT I CAN USUALLY GET TO A SERVER THAT'S HOSTING INTERNAL APPLICATIONS.
I CLICK ON **CITRIX** AND IT ASKS FOR MULTI-FACTOR AUTHENTICATION, SAYING IT'LL SEND IT VIA SMS* TO THIS USER'S CELL PHONE. BUT IT ONLY GIVES THE LAST FOUR DIGITS OF THE PHONE NUMBER. AND I ONLY HAVE SIXTY SECONDS TO AUTHENTICATE!
I TYPE IN THOSE DIGITS INTO THE SEARCH BAR WITHIN THIS PERSON'S E-MAIL AND I PULL UP ONE OF THEIR SIGNATURES THAT HAS THEIR FULL PHONE NUMBER.
*SHORT MESSAGING SERVICE
I CALL HER UP AND START RIGHT IN WITH THE COMPUTER GOBBLEDY GOOK.
HI, I'M WOODY FROM **I.T.** AND WE NEED TO MIGRATE YOUR CITRIX SINCE IT'S PLENA EST STULTITIA HO Bb! 3TOГO 3HAETE (f(x)±g(x))'= f'(x)±g'(x)
Uhhh, OKAY...WHY ARE YOU CALLING ME?
I'M GONNA SEND YOU A PIN NUMBER* THAT I NEED YOU TO READ BACK TO ME THAT AUTHENTICATES THAT THIS **IS,** IN FACT, YOUR ACCOUNT.
THAT'S IT? OKAY.
*TO RECAP. CITRIX WILL BE SENDING THAT TEXT, NOT ME.
SHE GOT CITRIX'S TEXT, READ IT TO ME, AND I TYPED IT IN WITHIN THE MINUTE--'CAUSE YOU ONLY HAVE ABOUT SIXTY SECONDS FROM WHEN THEY SEND IT--AND IT LOGGED ME IN.


BUT THERE ARE NO APPLICATIONS INSIDE CITRIX. NO COMPUTERS.
I'VE HACKED MY WAY INTO A BROOM CLOSET!
AT THIS POINT IF YOU WERE TO LOOK OVER AT "JEREMY FROM MARKETING" YOU'D SEE HIM SWEATING AND SHAKING.
GENERALLY, WHEN I'M DOING AN ATTACK, I'M CALM--ON THE OUTSIDE. INSIDE, ALL THE ANXIETIES ARE THERE, BUT IT'S NOT UNTIL AFTERWARDS, WHEN THE ADRENALINE RUSH CRASHES, THAT I KIND OF FALL APART A LITTLE.
I USED TO BE A SERGEANT IN THE MARINE CORPS!
AND WHEN YOU'VE GOT A PLATOON FULL OF TRAINED KILLERS AND YOU'RE TRYING TO GET THEM TO DO WHAT YOU WANT THEM TO DO, YOU HAVE TO DEVELOP CONFIDENCE--OR AT LEAST A PROJECTION OF CONFIDENCE.
YOU GOTTA LIE THROUGH YOUR TEETH, RIGHT? I WILL HAVE CONFIDENCE; I'M SOCIALLY ADEPT BUT IT STILL DRAINS ME--
ESPECIALLY WHEN I'M DOING SOMETHING LIKE THIS THAT I HAVE TO PUT ON A HEAVY MASK.

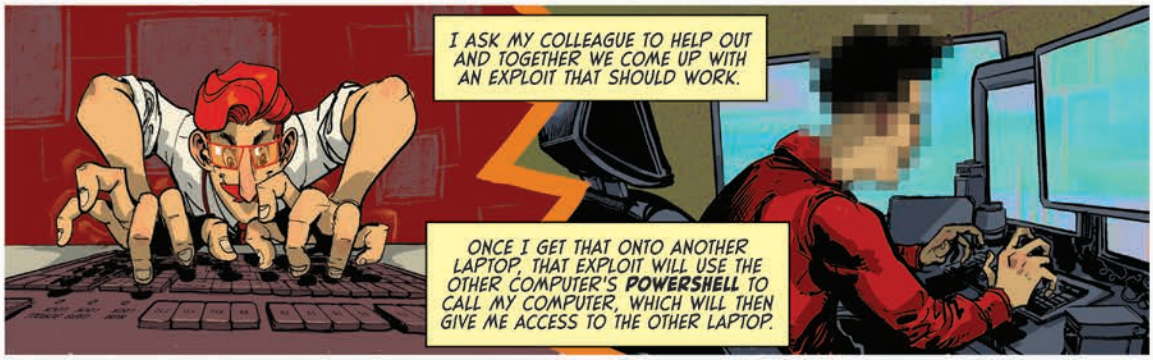

AFTER THIS, I GO "SCREW IT." I'M GONNA GO ALL OUT. AS PEOPLE START LEAVING TO HEAD HOME I SAY--
HEY, I'M GONNA STAY BACK AND FINISH UP.
AND NOBODY TOOK MUCH NOTICE.
I WAITED UNTIL THE CLEANING CREW CAME.
I WAITED UNTIL THE CLEANING CREW LEFT. UNTIL I WAS THE ONLY ONE ON THE FLOOR.
AND I HEADED STRAIGHT FOR THE I.T. SHACK. THIS IS WHERE LOADS OF COMPUTERS ARE KEPT AND THEY SHOULD GIVE ME ACCESS TO SOME OTHER WORKSTATIONS.
I WAIT RIGHT AROUND THE CORNER FROM THE I.T. SHACK ENTRANCE AND TRY TO LISTEN TO SEE IF ANYONE IS AROUND.
THIS LOOKS SILLY, BUT YOUR JAW MUSCLES PARTIALLY BLOCK YOUR EAR CANAL WHEN YOUR MOUTH IS CLOSED. OPEN YOUR MOUTH AND YOU JUST HEAR BETTER.
I TURN THE CORNER, WALK IN, AND I'M STANDING IN FRONT OF LIKE, SEVENTY-FIVE LAPTOPS OR MORE!


I ENDED UP GRABBING ABOUT THIRTY LAPTOPS BEFORE I SAID, "YOU KNOW WHAT? THIS IS PROBABLY ENOUGH."
THE IDEA IS TO SEE IF I CAN FIND ANY UNENCRYPTED HARD DRIVES IN THE BUNCH AND IF I CAN, I'LL DUMP THE LOCAL ADMINISTRATOR HASH FROM IT.
ONLY TWO OF THE LAPTOPS WERE UNENCRYPTED. BUT THAT'S ENOUGH.
I RUN THE HASH I GET THROUGH MY PASSWORD-CRACKING RIG AND I GET A PASSWORD RATHER QUICKLY. I TRY IT ON MY OWN LAPTOP, AND IT WORKS, WHICH MEANS IT'S LIKELY THAT'S THE ADMIN PASSWORD FOR ALL THE COMPUTERS IN THE OFFICE.
I GOT A LUCKY BREAK. BUT AFTER THIS DAY I'VE HAD, I'M BEAT AND I GO HOME AND I SLEEP.
FEELING RESTED, AND HAPPY THAT I HAVE AN ADMIN HASH AND A PASSWORD, I COME BACK IN THE NEXT MORNING FOR DAY THREE, READY TO DIG DEEP INTO THE NETWORK.
BUT THE PASSWORD I GOT WASN'T ALLOWING ME ACCESS TO OTHER HARD DRIVES AT THE USER LEVEL. IT COMES UP AS A VALID CREDENTIAL BUT YOU'RE NOT ALLOWED TO LOG IN.
"THIS IS ASININE!!"
IT TURNED OUT THAT THEY WERE USING A THIRD-PARTY NON-MICROSOFT TOOL TO DO ACCESS CONTROL AND USER CONTROL, ETC.


I'M TIRED OF FLYING UNDER THE RADAR, SO I SCAN MY OWN LAPTOP FOR VULNERABILITIES, AND THE ONE THAT I THOUGHT WOULD WORK WAS AN UNQUOTED SERVICE PATH.
SEE, SOME PROGRAMS RUN AUTOMATICALLY WHEN YOU START UP YOUR COMPUTER. BUT, SAY, ONE OF THE FOLDERS THAT YOU RUN THAT PROGRAM FROM HAS SPACES IN ITS NAME--LIKE BOGUS SERVICE.
NOW, UNLESS THERE ARE QUOTATION MARKS AROUND THE FULL PATH, WINDOWS WILL TRY TO RUN THE WORD UP TO WHERE THE SPACE IS--BOGUS, IN THIS CASE--
--AS AN EXECUTABLE BEFORE TRYING TO RUN BOGUS SERVICE AS A DIRECTORY.
SO, IF I WRITE A MALICIOUS PROGRAM NAMED SIMPLY BOGUS AND INSTALL IT ON ANOTHER COMPUTER, AS SOON AS A USER BOOTS IT UP, I CAN REMOTELY EXPLOIT THEIR LAPTOP.
I FOUND A DIRECTORY THAT LET ME DO THIS. GREAT, RIGHT?
BUT I RAN A CHECK TO SEE IF I HAD WRITING PRIVILEGES AND IT SAID I DIDN'T. EVEN IF I GET MY MALICIOUS PROGRAM ON ANOTHER LAPTOP, WITHOUT THE ABILITY TO WRITE TO THE REMOTE COMPUTER, I'M UNABLE TO EXPLOIT IT.
AT THIS POINT I'M LIKE WELL, #@!% IT. I'M DONE. THIS IS HORRIBLE.
I'M NOW WRAPPING DAY THREE AND STILL HAVEN'T GAINED ACCESS TO ANY COMPUTER--OUTSIDE OF MY OWN AND A COUPLE OF POWERED-OFF LAPTOPS FROM THE I.T. SHACK.
MRS. ROBOT
LAUNDROMAT
SUPER DUMP
MY REPORT AND FINDINGS SO FAR LOOK DISMAL. USUALLY BY NOW I'M DEEP INTO THE SYSTEM OF A COMPANY. THIS HAS BEEN THE HARDEST ASSIGNMENT I'VE EVER HAD.


THE NEXT MORNING I CALL UP AN ASSOCIATE OF MINE. I TELL HIM EVERYTHING I DID, BUT WHEN I RAN THE CHECK TO SEE IF I HAD PRIVILEGES, IT SAID I DID NOT HAVE WRITABILITY.
AND THEN HE SAYS--
DID YOU TRY IT ANYWAYS?


WAP!
DAMMIT! I JUST ASSUMED!
I WENT AHEAD AND TRIED TO WRITE TO IT AND I COULD. EVEN THOUGH WINDOWS CAME BACK AND TOLD ME I COULDN'T, I WAS ALLOWED TO WRITE.
AGAIN, THIS THIRD-PARTY SOFTWARE THAT RAN ALL THE ACCESS CONTROL, IT ALLOWED USERS TO WRITE EVEN THOUGH THE NATIVE WINDOWS DIDN'T. THE THIRD PARTY SUPERSEDED WINDOWS.


I ASK MY COLLEAGUE TO HELP OUT AND TOGETHER WE COME UP WITH AN EXPLOIT THAT SHOULD WORK.
ONCE I GET THAT ONTO ANOTHER LAPTOP, THAT EXPLOIT WILL USE THE OTHER COMPUTER'S **POWERSHELL** TO CALL MY COMPUTER, WHICH WILL THEN GIVE ME ACCESS TO THE OTHER LAPTOP.

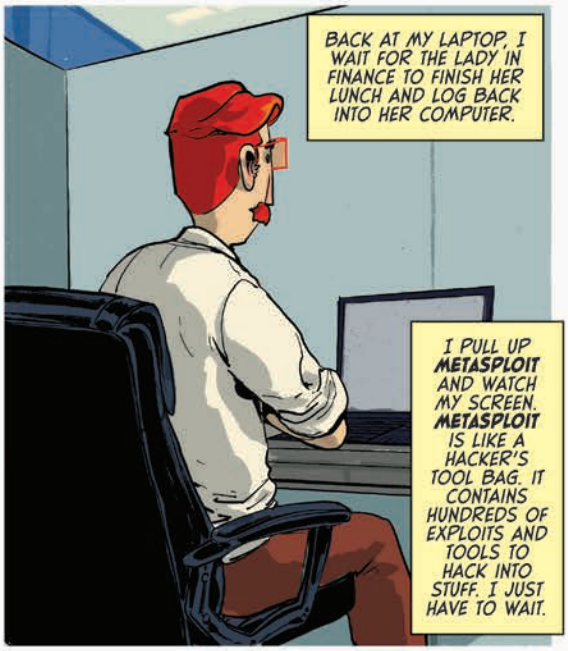

IT TESTS WELL ON MY OWN LAPTOP, UNPLUGGED FROM THE COMPANY DOMAIN, SO I DOWNLOAD THIS EXPLOIT ONTO A FLASH DRIVE.
NOW THE TRICK IS TO GET IT ONTO THE OTHER LAPTOP I WANT TO HACK BY UPLOADING IT FROM THIS USB DRIVE.


AND THE PLACE TO USE IT? **I.T.!**
WHEN EVERYBODY LEAVES FOR LUNCH, I GO STRAIGHT FOR IT. I'M GONNA HIT IT AND I'M GONNA TAKE THEM DOWN. I'M GONNA GET **SYSTEM LEVEL REMOTE ACCESS.**


WHEN I GET TO THE I.T. AREA, AND I CRAP YOU NEGATIVE, THE BULK MAJORITY OF I.T. ARE SITTING THERE EATING LUNCH AT THEIR DESKS.
THAT'S JUST NOT HEALTHY! THAT'S NOT GOOD WORK. YOU NEED TO GET AWAY FROM YOUR COMPUTER. YOU NEED TO STAND UP. YOU NEED TO WALK.
SO, I START WALKING, PACING AROUND. I MEAN, I'M LOSING MY COOL, BUT I'M STILL LOOKING FOR AN AREA WHERE EVERYONE ACTUALLY **IS** OUT TO LUNCH.
I GO AROUND A CORNER AND THERE IT IS.
I FINALLY FIND AN AREA THAT DOESN'T HAVE ANYBODY AND SURE ENOUGH IT'S **FINANCE.** I'M GONNA TAKE DOWN FINANCE!
BUT WHEN I GET CLOSER, I SEE ONE LADY SITTING IN ONE OF THESE CUBICLES EATING HER LUNCH.
STILL, I'M JUST GONNA GO FOR IT ANYWAY.
MOOLAND COW TAGE CHEESE
HI, I'M WITH **I.T.** AND I'M DOING SOME UPDATES IN THE OFFICE. CAN I WORK ON YOUR LAPTOP?
SOUNDS GREAT. GO AHEAD AND DO IT.


ONCE I'M AT THE DESK AND SHE'S NOT PAYING ATTENTION--

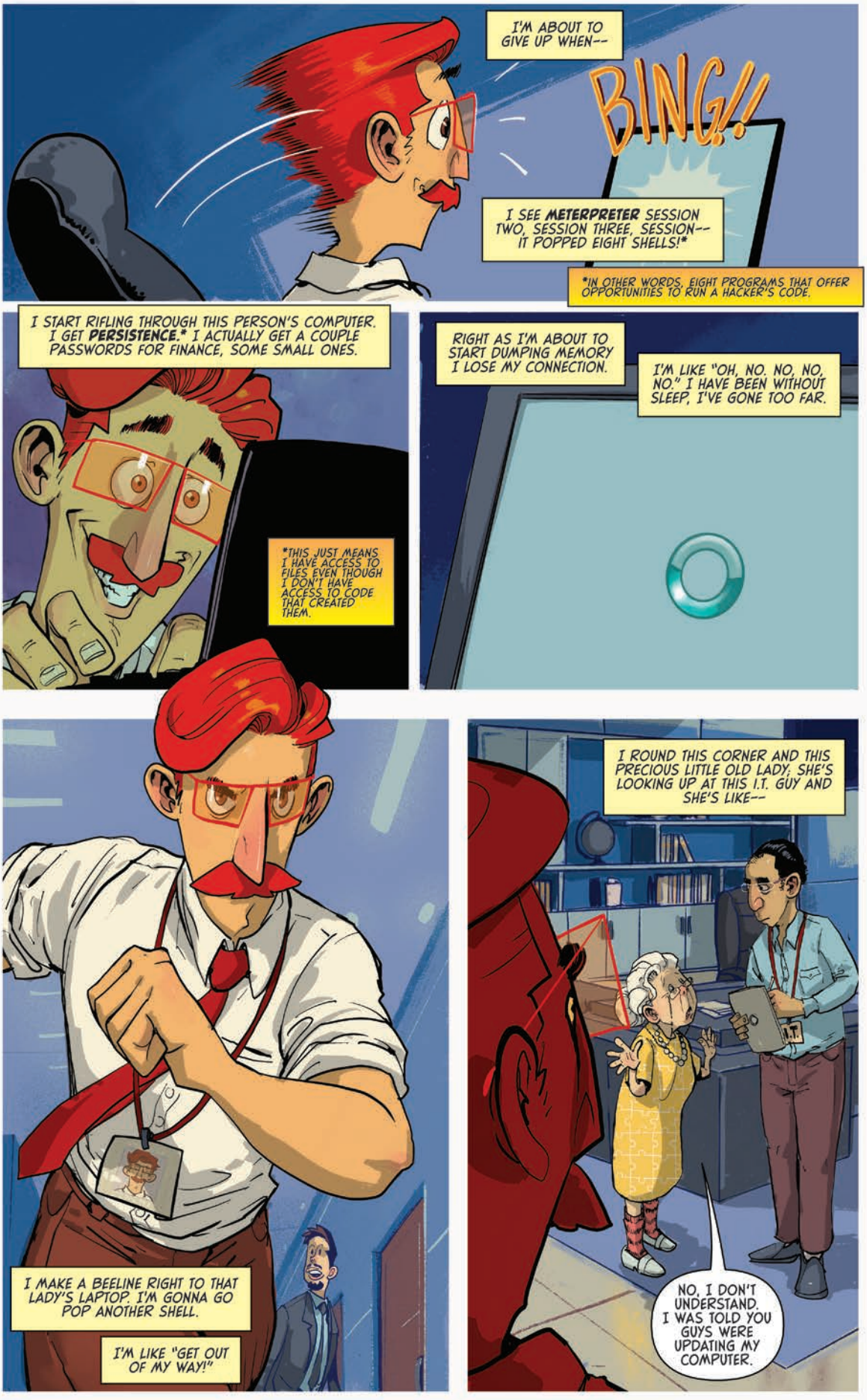

I POP IN THE USB DRIVE AND IT TAKES ME ABOUT THIRTY SECONDS TO LOG OUT, LOG BACK IN, DROP THE MALWARE INTO THE CORRECT FOLDER, LOG OUT AGAIN, AND I'M DONE.


BACK AT MY LAPTOP, I WAIT FOR THE LADY IN FINANCE TO FINISH HER LUNCH AND LOG BACK INTO HER COMPUTER.
I PULL UP **METASPLOIT** AND WATCH MY SCREEN. **METASPLOIT** IS LIKE A HACKER'S TOOL BAG. IT CONTAINS HUNDREDS OF EXPLOITS AND TOOLS TO HACK INTO STUFF. I JUST HAVE TO WAIT.


AND WAIT...


AND WAIT...


AND WAIT.
IT'S BEEN FORTY-FIVE MINUTES AND I BEGIN TO THINK IT JUST DIDN'T WORK.


I'M ABOUT TO GIVE UP WHEN--
BING!!
I SEE METERPRETER SESSION TWO, SESSION THREE, SESSION-- IT POPPED EIGHT SHELLS!*
*IN OTHER WORDS, EIGHT PROGRAMS THAT OFFER OPPORTUNITIES TO RUN A HACKER'S CODE.
I START RIFLING THROUGH THIS PERSON'S COMPUTER. I GET PERSISTENCE.* I ACTUALLY GET A COUPLE PASSWORDS FOR FINANCE, SOME SMALL ONES.
*THIS JUST MEANS I HAVE ACCESS TO FILES EVEN THOUGH I DON'T HAVE ACCESS TO CODE THAT CREATED THEM.
RIGHT AS I'M ABOUT TO START DUMPING MEMORY I LOSE MY CONNECTION.
I'M LIKE "OH, NO. NO, NO, NO." I HAVE BEEN WITHOUT SLEEP, I'VE GONE TOO FAR.
I MAKE A BEELINE RIGHT TO THAT LADY'S LAPTOP. I'M GONNA GO POP ANOTHER SHELL.
I'M LIKE "GET OUT OF MY WAY!"
I ROUND THIS CORNER AND THIS PRECIOUS LITTLE OLD LADY, SHE'S LOOKING UP AT THIS I.T. GUY AND SHE'S LIKE--
I.T.
NO, I DON'T UNDERSTAND. I WAS TOLD YOU GUYS WERE UPDATING MY COMPUTER.

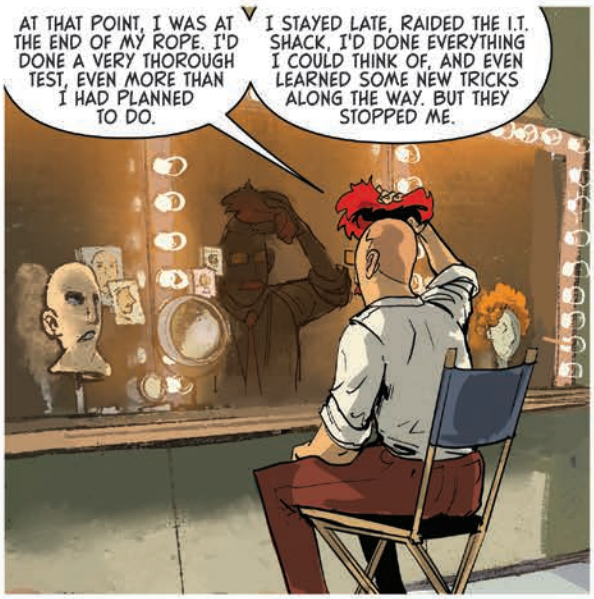

BUT WHEN SHE SEES ME--
IT WAS HIM!


I LET OUT THIS HIGH-PITCHED SEVENTH GRADE-GIRL SCREAM--
GAH!
AND RIGHT AS I TURN TO RUN...


BUSTED!
ISO
ISO


THEY SAT ME DOWN AND ASKED--
WHO ARE YOU? WHAT ARE YOU DOING WITH THESE COMPUTERS?
AND WHY ARE YOU CALLING YOURSELF I.T.?


WHEN A PENETRATION TESTER GETS CAUGHT LIKE THIS, THEY HAVE TO THINK. "SHOULD I TRY TO ESCAPE THIS SITUATION OR SHOULD I JUST TELL THEM I'M HERE WORKING FOR THE CISO?"
IN THIS CASE I DECIDED TO SAY--
I'M WORKING FOR THE CISO.


AT THAT POINT, I WAS AT THE END OF MY ROPE. I'D DONE A VERY THOROUGH TEST, EVEN MORE THAN I HAD PLANNED TO DO.
I STAYED LATE, RAIDED THE I.T. SHACK, I'D DONE EVERYTHING I COULD THINK OF, AND EVEN LEARNED SOME NEW TRICKS ALONG THE WAY. BUT THEY STOPPED ME.


THE CISO CAME IN AND EXPLAINED WHO I WAS AND WHY I WAS THERE.
HE WAS VERY HAPPY WITH THE RESULTS OF MY TEST, OBVIOUSLY. BUT HE DIDN'T GLOAT. THE GUYS IN SECURITY DIDN'T RUB IT IN. THEY WERE ALL VERY PROFESSIONAL, FROM THE TOP DOWN.


BUT I HAD TO ASK. I RAN THE SAFEST FRICKIN' SHELL THAT I COULD RUN. I EVEN TESTED IT AGAINST THEIR ANTIVIRUS AND THEIR ANTIVIRUS DIDN'T CATCH IT. I WAS ONLY THERE FOR THIRTY MINUTES.
HOW DID THEY FIND ME?


THEY SAID, "YOU WERE RUNNING POWERSHELL FROM A FINANCE COMPUTER AND FINANCE DOESN'T RUN POWERSHELL."
ONLY TECHNICAL PEOPLE EVER RUN IT OR NEED IT, LIKE I.T. AND MAYBE SOME OF OUR DEVELOPERS OR DEVELOPMENT OPERATIONS.


NOW LOOK, YOU CAN'T HAVE A PERFECTLY SECURE SYSTEM OR NO ONE'S GOING TO BE ABLE TO USE IT. IF SOMEONE CAN USE IT, AN ATTACKER CAN EMULATE THAT USER IN SOME FORM OR FASHION.
BUT THIS SYSTEM? I MEAN, IT WOULD TAKE AN ENTITY LIKE MOSSAD TO HACK IT. AND THAT'S A RISK ACCEPTANCE I THINK MOST COMPANIES CAN LIVE WITH.
I GUESS THAT'S IT. YOU SHOULD FOLLOW TINKER ON MASTODON BECAUSE HE TELLS A LOT MORE GREAT STORIES. HIS HANDLE THERE IS @TINKER@INFOSEC.EXCHANGE.
T.T.F.N.

TERMS!

PENETRATION TESTER | Page 1
Evaluates system vulnerabilities and tests defenses for clients.

RED TEAM | Page 1
Tests system security by emulating adversaries and understanding their attack methods.

CISO | Page 2
Chief Information Security Officer responsible for data and information system security.

DEFENSE IN DEPTH | Page 2
Multiple layers of defense to protect against threats.

RAM DASS | Page 3
Spiritual leader known for the quote, "The quieter you become, the more you can hear."

DNS | Page 5
Translates human-readable names to IP addresses on a network.

CLEAR TEXT PASSWORD | Page 6
Password stored or transmitted in a readable format without encryption.

AUTHENTICATION HASH | Page 6
Password transformed into an alphanumeric string using a hashing algorithm for authentication.

SUBNET | Page 6
Divided network using a subnet mask for control or performance improvement.

PASSPHRASES | Page 8
Complex passwords created by combining multiple random words.

MULTI-FACTOR AUTHENTICATION | Page 9
Requires multiple factors for user authentication.

IT SHACK | Page 12
Area where the IT team works and configures IT assets.

SYSTEM LEVEL REMOTE ACCESS | Page 15
Total control of a system from a remote location.

PERSISTENCE | Page 18
Establishing ways to maintain or regain access to a system if the original entry point is closed.

ISO | Page 19
Information Security Officer responsible for enforcing security controls and policies.

MOSSAD | Page 20
Israeli intelligence agency responsible for gathering intelligence and counterterrorism.

RISK ACCEPTANCE | Page 20
Accepting identified risks based on analysis and plans for monitoring and addressing them.

ATTACKS!

LIVING OFF THE LAND | Page 4
Attackers leverage existing tools and processes within the target environment to gather information and attack systems while avoiding detection and blending in with legitimate activity.

MASQUERADING | Page 4
Attackers capture network packets with Wireshark to masquerade as other systems by leveraging network information, while assigning penetration testing devices names and IPs to blend in on the network.

LLMNR POISONING | Page 5-6
Attackers leverage Responder to poison the LLMNR protocol, capturing authentication hashes by responding with incorrect information during local-link name resolution, similar to DNS.

HASH CRACKING | Page 7-8
Attackers analyze captured hashes, comparing them to a word list to determine valid passwords, facilitating unauthorized access through matching password hashes.

SOCIAL ENGINEERING | Page 10
Attackers impersonate IT, exploiting trust and providing a believable pretext for users to perform unauthorized actions, ultimately manipulating them to extract sensitive information.

CREDENTIAL DUMPING | Page 13
Attackers target unencrypted systems to perform credential dumping, focusing on locally stored credentials such as Local Admin or Administrator, exploiting the vulnerability of systems without Full Disk Encryption (FDE).

UNQUOTED SERVICE PATH | Page 14
Attackers exploit services with unquoted paths, utilizing the interpretation of spaces in paths without quotes as the end of the path, enabling them to execute malicious software and gain system-level privileges.

CUSTOM PAYLOAD | Page 15
Attackers develop tailored payloads to remotely access systems, leveraging user's computers to escalate privileges within the organization, while evading detection by utilizing a safe remote connection tool.

TOOLS!

UBUNTU
Popular user-friendly Linux based on Debian. Includes open-source software packages.

KALI LINUX
Specialized Linux for penetration testing. Based on Debian. Includes offensive security tools.

WIRESHARK
Packet capture tool for troubleshooting and information gathering.

CRACKING RIG
Specialized computer for cracking authentication hashes quickly.

HASHCAT
Software for discovering passwords by cracking hashes.

RESPONDER
Captures authentication from systems seeking resources for attackers to exploit.

METASPLOIT
Framework for automating vulnerability exploitation in penetration testing.

METERPRETER
Metasploit payload for controlling and accessing files on a target computer.

POWERSHELL
Automates system administration processes via a command-line interface.


HELLO AND WELCOME!
I'M JOHN STRAND, THE FOUNDER OF BLACK HILLS INFORMATION SECURITY.
I ALSO TEACH INFORMATION SECURITY TRAINING COURSES FOR ANTISYPHON TRAINING.
TODAY, I WANT TO SHARE WITH YOU THE WAYS THIS ORGANIZATION EXCELS IN SECURITY.
BLACK HILLS
INFORMATION SECURITY
DEFENSE-IN-DEPTH STRATEGY HINDERS NETWORK ACCESS AND LATERAL MOVEMENT FOR ATTACKERS.
LENGTHY PASSWORD POLICY CREATES DIFFICULTY FOR CRACKING ATTEMPTS.
LEAST PRIVILEGE PRINCIPLE LIMITS ACCESS RIGHTS, MAKING IT HARDER TO FIND ACCOUNTS WITH EXCESSIVE PRIVILEGES.
APPLICATIONS ARE SAFE-GUARDED WITH SINGLE-SIGN ON (SSO) AND MULTI-FACTOR AUTHENTICATION (MFA) FOR ADDED SECURITY AGAINST UNAUTHORIZED ACCESS.
I.T. AND SECURITY TEAMS ACTIVELY MONITOR FOR UNUSUAL BEHAVIORS, LIKE UNEXPECTED POWERSHELL CONNECTIONS, ALLOWING THEM TO IDENTIFY AND INVESTIGATE POTENTIAL THREATS.
THANKS TO TINKER AND JACK FOR LETTING US CREATE THIS COMIC THAT HIGHLIGHTS WHAT SECURITY TEAMS DO EVERY DAY TO HELP US STAY SECURE WHILE WE WORK.
BLACK HILLS

Remember – **Only YOU Can**
PREVENT BREACHES!

BEAR VS BEAR

REKCAHCOMICS.COM

ACTIVE COUNTERMEASURES

CTF

BRAND NEW TO THREAT HUNTING?

BRUSHING UP ON OLD SKILLS?

READY TO PROVE YOUR PROWESS?

Rise to the challenge with our ***exclusive*** Capture the Flag competition!

Custom built by ACM's very own Chris Brenton and Bill Stearns, test your mettle in this 25-question, threat hunting-based CTF, and earn the chance to win an **Active Countermeasures Threat Hunting coin!**

BLACK HILLS
Information Security
• 2008 •

Our top priority is helping you *understand and achieve* your security needs.

Specializing in:

- **Penetration Testing**
- **Red Teaming**
- **Active SOC**
- **Blue Team Services**
- **Purple Teaming**
- **Threat Hunting**
- **Incident Response**
- **Consulting**
- **Training**
- **IR Tabletop Exercises**

Clients include:

- Credit Unions
- Banks
- Investment Firms
- Higher Education
- Health Care
- Medical Devices
- Insurance
- Law Firms
- Real Estate
- Retail
- Technology
- IT
- Software
- Utilities
- ICS/SCADA

CONTACT US:

701-484-BHIS
consulting@bhis.co

www.blackhillsinfosec.com

These are true stories from the dark side of the internet.

This is a podcast about hackers, breaches, shadow government activity, hacktivism, cybercrime, and all the things that dwell on the hidden parts of the network.

This is Darknet Diaries.

www.darknetdiaries.com