The National Cyber League
A COMMUNITY WHERE CYBERSECURITY IS A PASSION

The 2020 NCL Comics
featuring Nine Cybersecurity Adventures
nationalcyberleague.org
WE'VE RECENTLY INTERCEPTED THIS PHOTO AND WE BELIEVE THIS IS THE LIBER8TION HACKER GROUP’S NEXT TARGET, BUT WE DON'T KNOW WHERE IT IS OR WHO WILL EXECUTE IT.

THERE'S A GOOD AMOUNT OF INFO HERE, LET ME SEE WHAT I CAN FIND ONLINE.

THERE'S HIDDEN METADATA INFORMATION IN PHOTOS THAT TELL US WHERE THE PHOTO WAS TAKEN.

I WAS ABLE TO FIND THEIR SOCIAL MEDIA ACCOUNT SINCE THIS PERSON USED THE SAME USERNAME.

... AND THEY TAGGED THEIR COFFEE SHOP LOCATION ON A POST, SO THIS WILL HELP US KNOW WHERE THEY'RE BASED AND NARROW IT DOWN.

YOUR OSINT SKILLS ARE AMAZING! WE CAN GET TEAMS IN PLACE TO PREVENT THIS ATTACK FROM OCCURING! THANK YOU!

JUST USING MY OSINT SKILLS FOR GOOD!

GETTING MY MORNING COFFEE!

COFFEE SHOP

@h4x0r
LOTS OF APPLICATIONS USE POOR CRYPTOGRAPHIC SCHEMES, SOME ARE WRONGLY IMPLEMENTED, SOME USE NONE AT ALL.

SOME SOFTWARE DEVELOPERS THINK IF THE DATA LOOKS RANDOM, IT’S SECURE, BUT THAT’S NOT ALWAYS THE CASE.

WE CAN LOOK AT THE FIRST FEW BYTES OF A STREAM, CALLED THE “MAGIC BYTES”, THAT USE THAT TO FIND THAT THE DATA STREAM IS JUST A BZIP2 COMPRESSED STREAM. IF WE JUST DECOMPRESS THE DATA STREAM, WE CAN FIND THE USERNAME AND PASSWORD.

THIS ISN’T AN ENCRYPTION SCHEME AT ALL, LET’S TAKE THIS BROKEN SCHEME AND REPLACE IT WITH AN ACTUAL SECURE ONE LIKE AES.
WE FOUND THE LIBER8TION HACKER GROUP’S BASE OF OPERATIONS BUT IT REQUIRES A PASSWORD TO OPEN THAT WE DON’T HAVE!

THERE’S THIS RANDOM SEQUENCE WRITTEN ON THE DOOR.

99fbe62390a9b0bb95bb2eee3f4bf6f7

INTERESTING... THIS IS A 32 CHARACTER SEQUENCE AND LOOKS TO BE HEXADECIMAL BASED ON THE CHARACTER SPACE HERE.

THIS IS LIKELY A HASH OF THE ACTUAL PASSWORD. HASHES ARE USED TO SECURELY SAVE PASSWORDS WITHOUT KEEPING THE ORIGINAL PLAINTEXT PASSWORD.

32 CHARACTER HEXADECIMAL REPRESENTS 16 BYTES OF DATA, OR 128 BITS, WHICH IS THE SIZE OF THE MD5 HASH DIGEST.

LUCKILY, I HAVE MY TRUSTY PAL, HASHCAT, THAT CAN CRACK HASHES LIKE THESE!

WE DID IT AGAIN!

THANK YOU AND HASHCAT FOR HELPING US CATCH THESE BAD HACKERS!
SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%

FRAUD ALERT!
CONFIDENCE: 52%

SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%

SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%

SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%

SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%

SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%

SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%

SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%

SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%
NCL Comic Series: Network Traffic Analysis

Hero eliminated known protocols - hacker foiled.

The hackers are using an unknown protocol!

Let me filter out these known protocols on Wireshark and write a custom dissector.

City Bank
Go @ 15:30

Your packet inspection skills saves the day again.
Forensics analysis finds hidden WiFi pineapple as source of breach.

Two weeks later:

Hero's Herald: Company WiFi breached by hackers.

Can I use your restroom please?
Sure, it's to the right.

Thanks for coming, we don't know how they got into the WiFi network.

How can I help chief?

Wells, looks like they're using a weak WPA passphrase, I was able to crack the passphrase in just seconds... and something else here looks fishy...

Let's see what WiFi network you're running here. I'll scan with Airwaves real quick with Airodump-ng... is... it in the bathroom...?

Look at what I found in here!

Looks like they were sniffering the WiFi traffic using this "WiFi pineapple".

Great work! We'll take it from here and find who planted this device!
WANTED SECURITY BUGS

ONCE WE WERE IN, THE ADMIN PANEL GAVE US A CUSTOMER SEARCH BAR THAT HAD ALL THE BILLING INFORMATION ON THE CUSTOMERS… AND WE FOUND A SQL INJECTION VULNERABILITY THAT ALLOWED US TO CHANGE THE BILLS OF THEIR CUSTOMERS.

WE IMMEDIATELY DISCLOSED THESE VULNERABILITIES TO THE CITY!
WE'RE GONNA NEED SOME HELP.

LET'S SEE IF THERE ARE ANY CONTAINERS LEAKING INFO...

HMM, THEY ANNOUNCED MIGRATION TO THE CLOUD AND USING DOCKER CONTAINER TECHNOLOGY, I WONDER IF IT'S GOT ANYTHING TO DO WITH THAT.

DOCKER CONTAINERS LAYER THEIR IMAGES, I SUSPECT THEY ACCIDENTALLY INCLUDED SENSITIVE INFORMATION IN HERE. IF WE CLOSELY INSPECT THE CONTAINERS, WE MIGHT FIND SOMETHING...

FOUND IT! API KEYS WERE EXPOSED IN THE CONTAINER HISTORY.

EVEN THOUGH THE IT DEPARTMENT TRIED TO REMOVE THE API KEYS AFTER THEY USED IT IN THE CONTAINER, THE DOCKER HISTORY WOULD STILL REVEAL IT. THEY SHOULD BE USING MORE SECURE KEY MANAGEMENT PRACTICES!

WE'RE GONNA NEED SOME HELP.
NCL Comic Series: Enumeration & Exploitation

How the fortress was saved.

OUR SERVERS ARE HARDENED AND FORTIFIED! WE WELCOME ALL PENTESTERS!

LET'S RUN SOME SCANS TO SEE WHAT YOU'VE GOT.

THIS IS A SERIOUS ROOT PRIVILEGE ESCALATION.

THANKS FOR SAVING OUR FORTRESS!