The National Cyber League
A COMMUNITY WHERE CYBERSECURITY IS A PASSION

The 2020 NCL Comics
featuring Nine Cybersecurity Adventures
nationalcyberleague.org
NCL Comic Series: Open Source Intelligence

Connecting the dots with OSINT.

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 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 OCCURRING! THANK YOU!

JUST USING MY OSINT SKILLS FOR GOOD!
NCL Comic Series: Cryptography

Magic bytes point the way.

Lots of applications use poor cryptographic schemes, some are wrongly implemented, some use none at all.

Qi Po07
FB W 32

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.

bzip2 magic bytes

username → password

42 5a 68 39 31 41

This isn’t an encryption scheme at all, let’s take this broken scheme and replace it with an actual secure one like AES.
NCL Comic Series: Password Cracking

Hashcat heroine cracks password problem.

WE FOUND THE LIBERATION 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.

9f9be62390a9b0bb5bb2ee3f4bf6f7

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

plaintext → ⇢

★ ★ ★ ★ ★ ★ ★

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!
NCL Comic Series: Log Analysis

Lead SOC analyst injects order, solves case.

SECURITY OPERATION CENTER (SOC)

FRAUD ALERT!
CONFIDENCE: 52%

SIR, SHOULD I MAKE THE CALL?
MAKE THE CALL.

LEAD SOC ANALYST

THIS IS TOO MUCH UNSTRUCTURED DATA, WE CAN'T CORRELATE ALL OF THIS TOGETHER.

WE'LL NEED TO FEED THIS INTO A SIEM SYSTEM OR A LOG ANALYZER.

WE'LL WORK ON TURNING THESE INTO STRUCTURED DATA SO WE CAN FEED IT INTO THE SYSTEM BETTER.

IP: 91.37... UNSTRUCTURED

PAYMENT...

ORDER → IP → PAYMENT → FRAUD

NOW WE CAN ORGANIZE THE DATA IN THE ORDER THAT THEY OCCURRED AND CORRELATE WITH EACH OTHER, THIS MAKES FINDING THE FRAUDSTER MUCH EASIER.

WE GOT THEM!
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.

YOUR PACKET INSPECTION SKILLS SAVES THE DAY AGAIN.
NCL Comic Series: Wireless Access Exploitation

Hackers hide pineapple in bathroom, breach company WiFi.

CAN I USE YOUR RESTROOM PLEASE?
SURE, IT’S TO THE RIGHT.

TWO WEEKS LATER

HOW CAN I HELP CHIEF?
THANKS FOR COMING, WE DON’T KNOW HOW THEY GOT INTO THE WIFI NETWORK.

WELL, 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 SNIFFING THE WIFI TRAFFIC USING THIS “WIFI PINEAPPLE”

GREAT WORK! WE’LL TAKE IT FROM HERE AND FIND WHO PLANTED THIS DEVICE!
NCL Comic Series: Web Application Exploitation

Weak admin login unlocked entire billing data.

WE STARTED OFF WITH A PRETTY NORMAL WEB APP, BUT QUICKLY FOUND MANY VULNERABILITIES.

I FOLLOWED THE ADMIN LOGIN LEAD AND FOUND....

...FOUR-DIGIT LOGIN PIN FOR THE ADMIN PANEL, IT WAS TRIVIAL TO GUESS.

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!
NCL Comic Series: Scanning
Docker container reveals all.

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

WE’RE GONNA NEED SOME HELP.

LETS SEE IF THERE ARE ANY CONTAINERS LEAKING INFO...

ACROSS TOWN

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!
NCL Comic Series: Enumeration & Exploitation

How the fortress was saved.

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

LETS RUN SOME SCANS TO SEE WHAT YOU’VE GOT.

THIS IS A SERIOUS ROOT PRIVILEGE ESCALATION.

THANKS FOR SAVING OUR FORTRESS!