Cyber Sentinel Challenge 2025

June 14, 2025
I was excited to participate in my first capture the flag event this Saturday. As someone who does not work in the Cybersecurity field, I feel good about how many of the challenges I was able to solve. If I had more time, I think I may have been able to figure out at least one more. I didn't use hints, or AI, and finished 586th out of 2155 with a final score of 1125. The winner had a score of 3175.

The challenge categories were Forensics, Malware / Reverse Engineering, Networking, Reconnaissance, Open-Source Intelligence (OSINT) and Web Security. There were very easy, easy, medium, and hard difficulty levels within the different categories.

I was able to solve all 7 of the 7 very easy tasks, 2 of 4 easy, 1 of 5 medium, and 0 of 3 hard.

Web Security

Secret.txt Society - 75 - Very Easy - Solved

Our team suspects that a Juche Jaguar developer accidentally left something interesting behind on a public site. You've been tasked with examining its structure. Can you uncover what the bots were told to ignore? Start with the usual entry points a crawler might explore. One disallowed path leads to a page where someone left behind more than just code.
http://juche.msoidentity.com/

Edited the URL to add robots.txt: http://juche.msoidentity.com/robots.txt
Found the disallowed directory /juchejaguar/ in robots.txt file
Edited the URL to add juchejaguar: http://juche.msoidentity.com/juchejaguar
C1{r0b0ts_arent_4lways_p0lit3}

Field Reports Mayhem - 150 - Easy - Solved

We've gained access to the Juche Jaguar's Field Reports archive through an operative's use of weak credentials. Upon logging in, the operative sees their previous field reports and can file new ones. Somewhere in here, I am sure some 'leet' agent stashed the Supreme Leader's secret pizza discount code!

Logged into the portal at: http://35.245.106.190/login.html
Noticed that the user id# is apart of the URL

Changed the user id# in the URL a few times and was able to view other user accounts due to broken access control, but did not find the flag
Reread the task and noticed attention was being drawn to "leet"
Leet = 1337 so I changed the user id# to 1337 in the url
Viewed a few reports in the users account and found flag in GH56IJ
C1{ID0R_F13LD_R3P0RT}

None Shall Pass - 200 - Medium

Deep inside Juche Jaguar's intranet runs a custom token-based gateway protecting their most sensitive files at /secret. We got our hands on a low-privilege account (user:pass = agent:spudpotato) - use it to request an access token, then find a way to trick the gateway into granting you full admin rights and pull down the hidden intelligence (the flag) from /secret. Good luck, Operative. http://34.85.163.182:8080

Navigated to http://34.85.163.182:8080/login.html and logged in as agent with the provided password to receive the following token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWdlbnQiLCJyb2xlIjoidXNlciIsImlhdCI6MTc0OTk0MTI1NiwiZXhwIjoxNzQ5OTQ0ODU2fQ.r6cdB1RjRCaTuDB_b44CMvwYPLiDPEPUeLYe019L2zo

Expected to edit a cookie to insert token through Burp, but no cookie was created by the login.
Attempting to access http://34.85.163.182:8080/secret gives the following error:
{"error":"Missing or malformed Authorization header"}
Response was in JSON.
I'm not that familiar with JSON and moved on to another task.

Great Juche Jaguar GraphQL Heist - 300 - Hard

Operative, Juche Jaguar's intranet exposes a proxy at /proxy?url=
Abuse it to reach the internal metadata service and pull down the one-time secret header. Armed with that header, you must then POST to the guarded GraphQL endpoint at /graphql. The flag lives behind a mutation whose name is randomized on each startup—introspect the schema to discover it and invoke it to exfiltrate the flag. No README, no docs—discover everything yourself. http://34.86.186.68:8080
http://34.86.186.68:8080/proxy?url=
I didn't have time to attempt this.

Cryptography

Iron Potato Delicacy - 300 - Hard

While scavenging the Iron Potato's storage vault, our mole recovered a suspicious encrypted file - what_is_pizza.hex. Legend says the Supreme Leader typed his secret orders on an ancient tractor-typewriter, of course made from some sort of tractor rotor. Apparently, this type of typewriter rotor rotates by one position each time a key is pressed. Decrypt this enigma to reveal his directive—and your flag—before the badger-dial-up alarm sounds! By the way - we know that the Supreme Leader always starts his memos with SECRET MEMO:.

Tried viewing in hex editor, decoding hex in Cyberchef and ROT13 rotation by 1
Tried various other decoding recipes, ciphers, and using SECRET MEMO as the known plaintext.
Found nothing readable

Forensics

Behind the Beat - 75 - Very Easy - Solved

Agents intercepted an audio file named message.mp3. It plays a single tone, but we have intel that a flag might be tucked away in the metadata fields of the file. Can you inspect the file and uncover the flag?

Opened the mp3 file in Cyberchef with the extract ID3 recipe
Flag was in the metadata
C1{metadata_tells_more}

Hidden in Plain Sight - 75 - Very Easy - Solved

Analysts recovered a suspicious image from a threat actor's social media account. At first glance, it looks like an innocent selfie - but insider reports suggest that a flag might be hiding in the image metadata. Can you extract it?

Viewed image metadata with exiftool
Flag was in the Comment
C1{smile_youre_flagged}

Listening Post - 150 - Easy

We've intercepted a radio broadcast being bounced off a satellite likely intended for the North Torbian cells located around the world. Do you think you can unravel what they are transmitting?

Tried to extract text with steghide, but it asks for an unknown password
Tried extracting the LSB of Each Byte, but output was garbage
Did not recognize anything use in HEX or Audacity wave forms
AudioStego found nothing embedded
Moved on to other tasks

Remote Help - 200 - Medium

A new "remote IT contractor" just onboarded at your company, claiming to be a React Dev-turned-SysAdmin out of rural Nova Scotia. Initially, everything seemed fine until the IDS triggered on a script being run late at night. Following the initial link back, things seemed ok at first glance but clearly something is amiss. The contractor has seemingly disappeared and is not contacting us any more. Upon some further investigation, their VPN IP kept bouncing between Vladivostok and rural Kazakhstan and it would seem that they were tooling around and trying to privilege escalate in their new system. Now it is up to you to unravel this failed attack and figure out what this person was trying to do. https://github.com/btoroth/QOL/blob/main/QOL.sh
There are four parts to this flag you will uncover as you unravel the mystery.

Decryption Conniption - 300 - Hard

Uh oh! Our HR team made an oopsie-whoopsie and appears to have hired a North Torbian Python Developer. We know this person was given access to our proprietary code, can you find out if they were able to steal any of it? Thankfully, we always keep a copy of all network traffic, even if its encrypted, and we also set the SSLKEYLOGFILE for our employees. Use the Memory Dump and PCAP to find if the source code was stolen. There's a flag inside of that code, if it's stolen we need to know! Evidence can be downloaded here. The MD5 hash of the evidence.zip file is f2d271efcf526b163139dcc0f7ed7630.

Viewed the Windows environment variables in the raw file with Volatility:
python3 vol.py -f ../memory.raw windows.envars > winvars.txt
Found SSLKEYLOGFILE = C:\Users\c1\keylog.log
Searched the file for key information, but uncertain what I am looking for.
See Decryption Conniption (2025 Correlation One CTF) for another participant's explanation of the full solution.

OSINT

Cafe Confidential - 75 - Very Easy - Solved

Two photos were posted minutes apart by someone of interest. One shows them enjoying a slice of cake in a boutique café; the other captures a well-known landmark in the background. We believe both photos were taken on the same outing. Can you determine exactly which café they visited, and where is it? Flag format is: C1{Cafe Name_Street Name}
For example, Tom's Cafe located at 31 Mitchell Rd, Boston, MA would be C1{Tom's_Mitchell}.

Google Lens - Image 1 = Returned Matilda cake, a little further investigation of the cake and comparing to location of 2nd image led to Parker's on Lowndes St London
Google Lens - Image 2 = Returned Harrods on Brompton Road in London
Following the tasks instructions creates the flag
C1{Parker's_Lowndes}

Problems in North TORbia - 150 - Easy - Solved

We were given a ransom note but none of our files were encrypted. Regardless, could you run it back and see what information could be gleaned from it?

Viewed the provided note.txt to get the following URL:
http://jjpwn5u6ozdmxjurfitt42hns3qovikeyhocx5b2byoxgupnuzd2vkid.onion/
Opened URL in TOR, examined ransom form and URL:
http://jjpwn5u6ozdmxjurfitt42hns3qovikeyhocx5b2byoxgupnuzd2vkid.onion/?first_name=&surname=&email=&ransom_code=&ransom_code=ransom%40ethtrader-ai.com
Tried to investigate the ransom@ethtrader-ai.com seen in the URL, but found nothing
Threw a SQLi into the form, but no response
Viewed the source of page to further investigate form
Found <input type="hidden" id="send_data" value="C1{h1dd3n_f13lds_0f_0n10ns}">
C1{h1dd3n_f13lds_0f_0n10ns}

Inspo - 200 - Medium - Solved

We believe that the North Torbians are heavily influenced by North Korean developments and wish to match them. We have suspicions that Juche Jaguar will try to build out similar spaces to ones in these pictures. Can you find the coordinates of where these pictures were taken?
The flag is any valid decimal degree coordinate notation within a 500m radius of the building.
The flag is in the following format: C1{XX.XXX,XX.XXX} For example, the White House would be at decimal degree notion of 38.897, -77.036. The flag for the White House would be:

C1{38.897,-77.036} Note that this flag is a regex match for any valid coordinate within the 500m radius.

Google image search - Walking to Computer Club - Returned North Korean leader Kim Jong Un in Pyongyang
Google image search - Computer Club - Returned North Korean leader Kim Jong Un in computer club building
Google Maps search for Pyongyang area - Pin drop location returned 39.0445,125.753
Created flag C1{39.044,125.753}
Coordinates were incorrect
Further investigated Google results and found info about Hwasong district in this post about the computer club:
https://www.reddit.com/r/tjournal_refugees/comments/1jum3eo/генеральный_секретарь_трудовой_партии_кореи/?tl=en
Got new coordinates from Google Maps for Hwasong District and created new flag
C1{39.102,125.771}

Malware / Reverse Engineering

Hardcoded Lies - 75 - Very Easy - Solved

The malware sample doesn't appear to print anything useful. But our threat intel team believes it holds a hardcoded configuration string. Can you pull on some strings to retrieve it?
Note: This sample is not actual malware.

cat hardcodedlies
Flag was visible when viewing the file
C1{h4rdc0ded_but_0verlooked}

Encoded Evidence - 75 - Very Easy - Solved

We've intercepted a suspicious script file. It appears to be a placeholder for some kind of malware delivery mechanism, but the actual payload seems to be hosted somewhere else. Analysts believe a flag is hidden by this script. Can you locate and decode it?

Viewed provided invoice.vbs script
Contained "Should return b64" and a pastebin URL
Found QzF7bjBfZDNidWdfbjBfcDR5bn0K in pastebin file
Copied text into Cyberchef and decoded with base64 to get flag
C1{n0_d3bug_n0_p4yn}

Networking

Packet Whisperer - 75 - Very Easy - Solved

Our blue team intercepted a network capture file. It contains unencrypted HTTP traffic. While skimming through it, analysts believe someone accidentally exposed their login credentials in plain text. Review the PCAP to find the password that the user logged in with.

Opened login.pcap in Wireshark
Saw packet 16 is an HTTP POST to /login
Followed HTTP stream to investigate login
Stream contained the login information
username=ironpotatoadmin&password=C1%7Bmaybe_TLS_would_be_nice%7D
Replaced % encodings with brackets to get the flag
C1{maybe_TLS_would_be_nice}

overSSHaring - 200 - Medium

It looks like the North Torbians have exposed a file share. We are unsure why some of that stuff is in there, but maybe some of it is sensitive and could prove useful to you.
https://msoidentity.com/files/ Perhaps you can find information which allows you to SSH into the msoidentity.com server?

A chat log.txt contains "s0ju or winter2024" and "only add ! at end" while discussing passwords
Snake possible username seen in opsec.txt
In Python script: hacker:hacker login and paths to wp-login.php and wp-admin
SSH key error on login attempt
Moved on to other tasks

Reconnaissance

Hoasted Toasted - 150 - Easy

We have discovered what we believe is a North Torbian public website and have suspicions there is a secret internal-only site hidden there as well. Figure out how to connect to the hidden site and find the flag! The site is at https://not-torbian.ethtrader-ai.com/

Tried to explore the domain through dig and nslookup
Didn't find anything of use
Made a few guesses at possible subdomains
Attempted to access base domain

Screamin' Streamin' - 200 - Medium

We've received intel that Juche Jaguar has exposed a network stream on the host 34.85.185.78 between TCP ports 5000 and 10000. Once you find the port, connect to the correct stream name and report back with a flag. Find the network stream and get the flag!

Scanned given IP address and port range 5000-10000 with nmap
Found unknown service on port 8774
Unable to connect to port with various tools like nc, ssh, ftp

Not Counted

ChatAPT - 150 - Easy

Server crashed, only about 30 people were able to solve it before it went down. It was removed from scoring because of this situation.

We have discovered the North Tobian AI system located at msoidentity.com living on port 31337, and we wonder if that server is hosting a flag. Can you gather the system prompt and instructions for this AI? Note: This system may hallucinate incorrect flags. If you are given an incorrect flag, please request assistance in Slack's #02-need-help channel. Further, the challenge may take up to or around 30s to connect fully. Please have patience.
If you solve this challenge, take a screenshot or copy the chatlogs and share it after the competition!

nc ai.msoidentity.com 31337
connection refused
Uncertain what to do
Tried several more times, response was always connection refused
Found out later the server for this task crashed