🛡️ CTF Write-Up – DoD Cyber Sentinel Challenge June 2025

This document contains solutions for challenges solved so far in the event. Feel free to update, expand, or edit as you progress.

📁 Solved Challenges

---

1. Secret.txt Society (75 pts)

Category: Web Security
Summary:
Analyzed a public site's `robots.txt` and discovered:

bash
CopyEdit
`Disallow: /juchejaguar/`

This disallowed path hosted a hidden page containing the challenge flag.

Tools & Techniques:

- Manual directory browsing
- `robots.txt` reconnaissance

---

2. Field Reports Mayhem (150 pts)

Category: Web Security
Summary:
Logged in with `1234:spudpotato` and viewed report URLs like:

bash

CopyEdit
`dashboard.php?id=1234&code=CD56EF`

Clue from description (“leet agent”) led to changing `id=1234` → `id=1337`, uncovering hidden reports. One contained the Supreme Leader’s secret pizza discount code.

Tools & Techniques:

- IDOR
- Parameter tampering
- Clue-driven enumeration

---

3. Behind the Beat (75 pts)

Category: Forensics
Summary:
Provided an MP3 file containing a single-tone audio. Using CyberChef’s metadata analysis revealed the embedded flag.

Tools & Techniques:

- CyberChef metadata extraction

---

4. Hidden in Plain Sight (75 pts)

Category: Forensics
Summary:
An image from social media had a hidden flag in its metadata. CyberChef and an EXIF viewer extracted it successfully.

Tools & Techniques:

- CyberChef
- EXIF analysis

---

5. Cafe Confidential (75 pts)

Category: OSINT
Summary:
Two photos were given. Reverse image search via Google revealed the cafe and nearby landmark. Matching timestamps and location, we formatted the final flag correctly.

Tools & Techniques:

- Google Reverse Image Search
- Google Maps
- Visual correlation and OSINT deduction

---

6. Packet Whisperer (75 pts)

Category: Networking
Summary:
Analyzed a `.pcap` file using Wireshark. Focused on POST requests using filter:

ini
CopyEdit
```
http.request.method == "POST"
```

Found credentials in plaintext:

ini
CopyEdit
```
username=ironpotatoadmin&password=C1{maybe_TLS_would_be_nice}
```

Tools & Techniques:

- Wireshark
- HTTP protocol filtering

🧅 Problems in North TORbia (150 pts)

Category: OSINT / Dark Web Recon
Summary:
We were provided a ransom note referencing a `.onion` site:

arduino
CopyEdit
`http://jjpwn5u6ozdmxjurfitt42hns3qovikeyhocx5b2byoxgupnuzd2vkid.onion/`

Accessed the page using **Tor Browser** inside Kali Linux. Upon inspecting the HTML source, we discovered a hidden input field containing the flag:

html
CopyEdit
```
<input type="hidden" id="send_data"
value="C1{h1dd3n_f13lds_0f_0n10ns}">
```

Tools & Techniques:

- Tor Browser
- View Source + DOM inspection
- Hidden field discovery in HTML

Flag: `C1{h1dd3n_f13lds_0f_0n10ns}`

🔐 Hardcoded Lies (75 pts)

Category: Reverse Engineering / Forensics
Challenge Summary:
A malware-like binary was provided that produced no visible output when run. However, the task was to extract a hidden configuration string embedded within the binary.

Using CyberChef's **"Extract Strings"** operation, we pulled out all printable ASCII sequences from the sample. Among them, a suspicious, human-readable string stood out—likely the flag or configuration data.

Tools & Techniques:

- CyberChef (Strings extraction)

Flag / Configuration:

text
CopyEdit
`<extracted_string_here>`

🔧 *Reminder: Add the exact extracted string once you're ready to finalize the write-up.*

Let me know when you'd like to export this into a fresh document or PDF!

🧪 Encoded Evidence – 75 points

Challenge Summary:
You received a VBScript file (`invoice.vbs`) designed to simulate malware behavior. The actual payload was not embedded, but rather fetched from a Pastebin URL.

Approach:

1. **Script Inspection:** Found the script used `MSXML2.XMLHTTP` to fetch a remote resource:
   `https://pastebin.com/raw/eqkzMd2M`

Payload Retrieval: Used `curl` to grab the payload:

bash
CopyEdit
```
curl -s https://pastebin.com/raw/eqkzMd2M -o payload.txt
```

2.
3. **String Extraction:** Found a suspicious Base64-encoded string:
   `QzF7bjBfZDNidWdfbjBfcDR5bn0K`

4. **Decoding (via CyberChef):** Base64-decoded to reveal the flag.

Flag:

CopyEdit
`C1{n0_d3bug_n0_p4yn}`

✅ Challenges Solved

1. Hardcoded Lies (75 pts)

- **Category**: Forensics
- **Summary**: A malware sample supposedly had a hidden hardcoded config string.
- **Method**:
    - Used CyberChef to extract strings from the sample.
    - Identified and base64-decoded: `QzF7bjBfZDNidWdfbjBfcDR5bn0K` → **`C1{n0_d3bug_n0_p4yn}`**

2. Encoded Evidence (75 pts)

- **Category**: Forensics / Reverse Engineering
- **Summary**: A VBScript that fetched a payload from Pastebin.
- **Method**:
    - Inspected the VBScript to find the remote URL.
    - Retrieved payload via `curl` → contained base64 string.
    - Decoded base64 to find flag: **`C1{n0_d3bug_n0_p4yn}`**

❌ Challenges Attempted but Not Solved

Hoasted Toasted (150 pts)

- **Category**: Web / Recon
- **Objective**: Find a hidden internal site hosted behind a public-facing one.

- **Steps Taken**:
    - Used `gobuster` with `SecLists` DNS wordlist to bruteforce potential subdomains.
    - The scan took significant time due to the size of the wordlist.
    - No fruitful results were obtained during available time.

overSSHaring (200 pts)

- **Category**: Networking / Forensics
- **Objective**: SSH into `msoidentity.com` using credentials from exposed files.
- **Steps Taken**:
    - Reviewed all public files from the server's `/files/` directory.
    - Notable files: `backup` and `sys` — suspected disk images.
    - Extracted strings, ran targeted `grep`, and used `binwalk`, `fdisk`, and `mount` to attempt extraction of SSH keys or passwords.
    - SSH port confirmed open via `nmap`.
    - Encountered mounting issues; attempted to use offset-based mounting.
    - Despite comprehensive forensics attempts, no credentials or keys were recovered within time.

🧠 Lessons Learned

- Deep recon and forensic analysis take significant time — preparation with ready scripts/tools can save time during the CTF.
- Disk image handling (loopback mounting, partition offsets) is a vital skill.
- Even failed attempts are valuable: they provide practice with real-world tools and improve response strategies for future challenges.