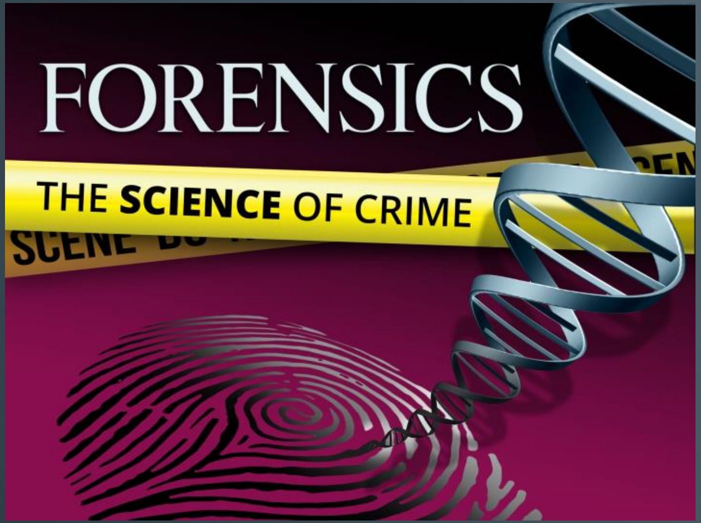
CHALLENGES DE FORENSICS RÉSEAU

POLYCYBER – MARS 2023

SAMUEL COUVRETTE

FORENSICS


FORENSICS
THE SCIENCE OF CRIME
SCENE

BIFURCATION
CORE
THE DELTA IS WHERE RIDGES

DIGITAL FORENSICS

> “**Digital forensics** is a branch of forensic science that focuses on *identifying, acquiring, processing, analysing, and reporting* on **data stored electronically**.
>
> Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations.
>
> Electronic evidence can be collected from a **wide array of sources**, such as *computers, smartphones, remote storage, unmanned aerial systems, shipborne equipment, and more.*”
>
> – Interpol

“ **Di**

ac

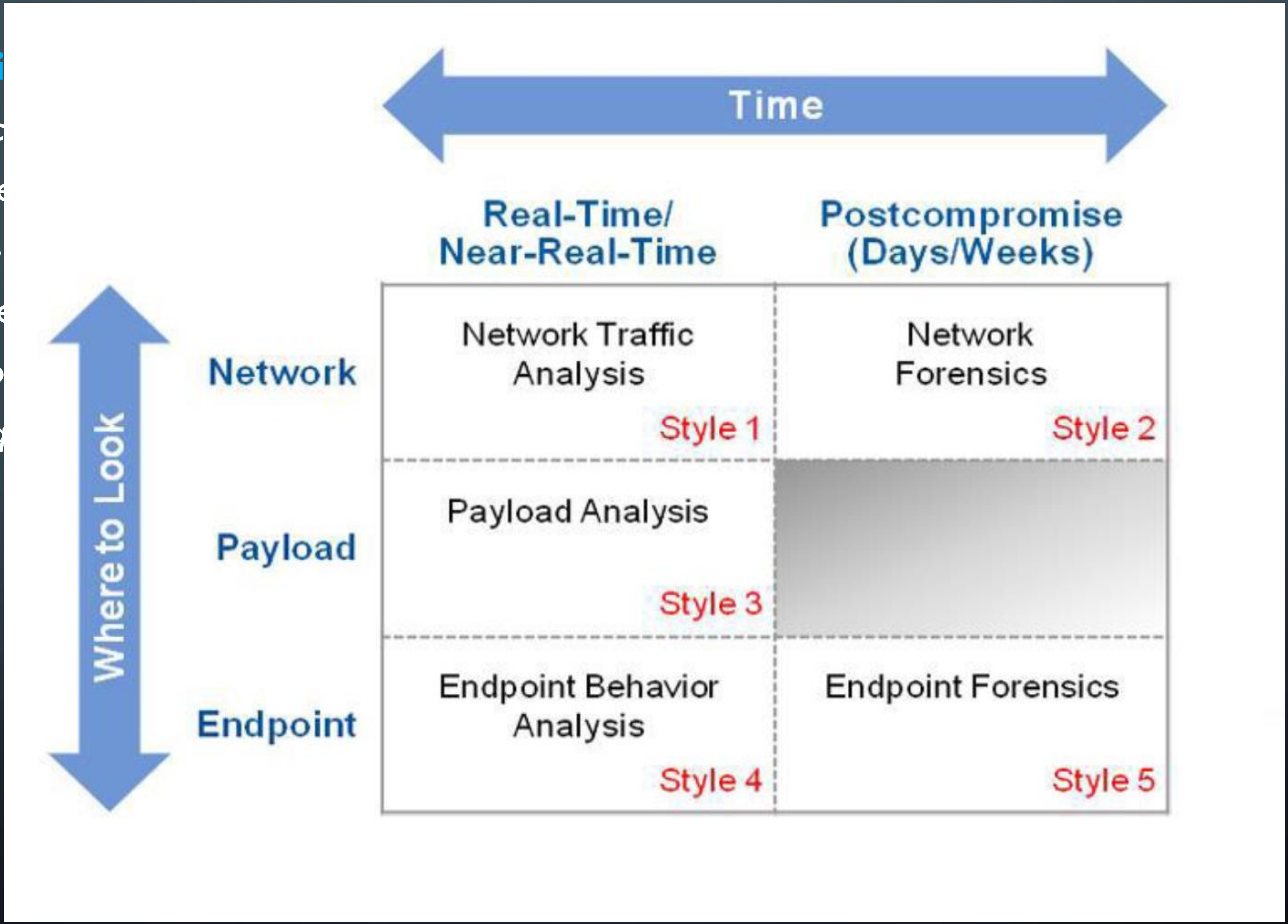
Ele

fo

Ele

co

eq ”



	Real-Time/ Near-Real-Time	Postcompromise (Days/Weeks)
Network	Network Traffic Analysis Style 1	Network Forensics Style 2
Payload	Payload Analysis Style 3	
Endpoint	Endpoint Behavior Analysis Style 4	Endpoint Forensics Style 5

“ **Di**

ac

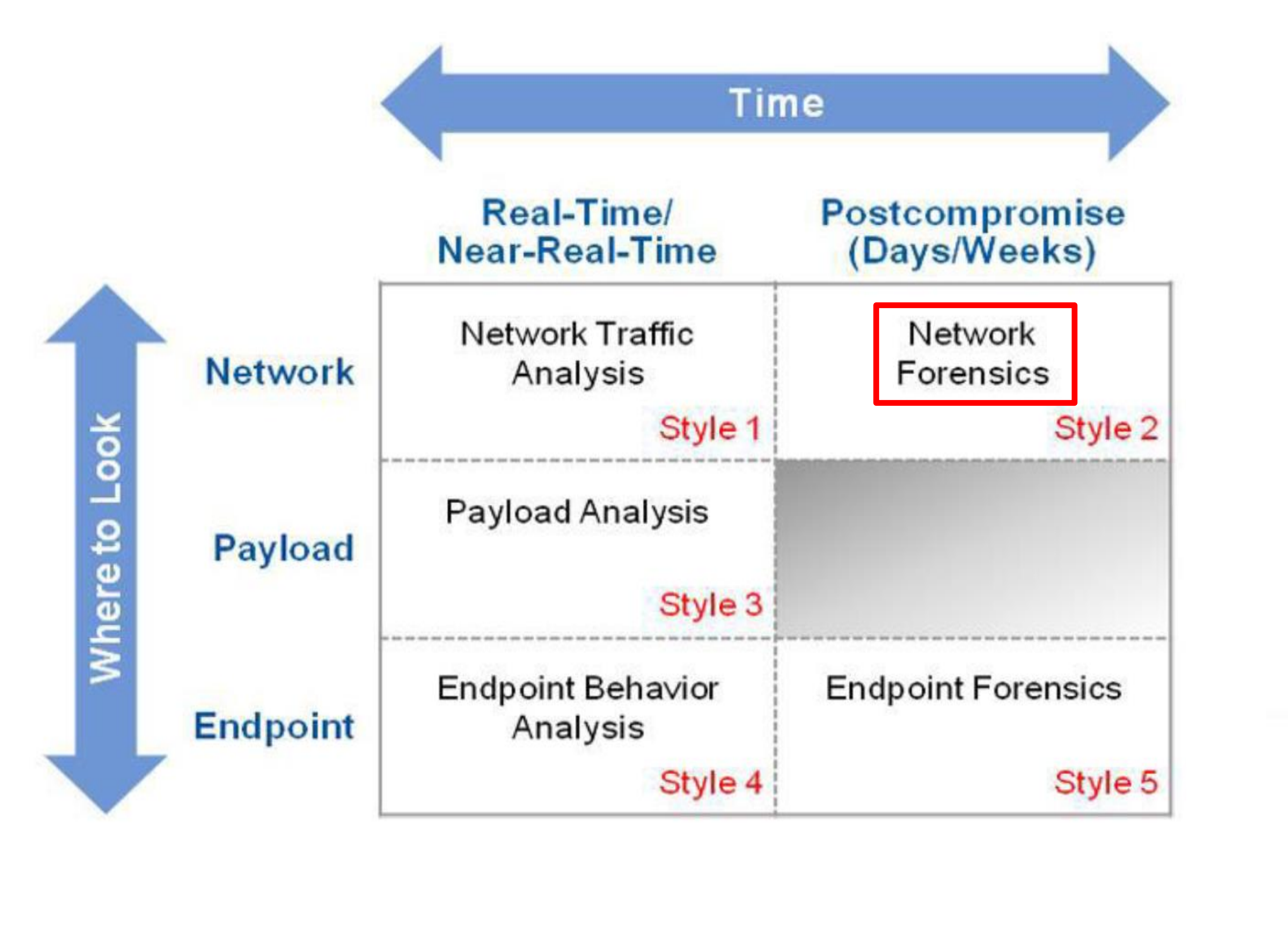
Ele

fo

Ele

co

eq ”



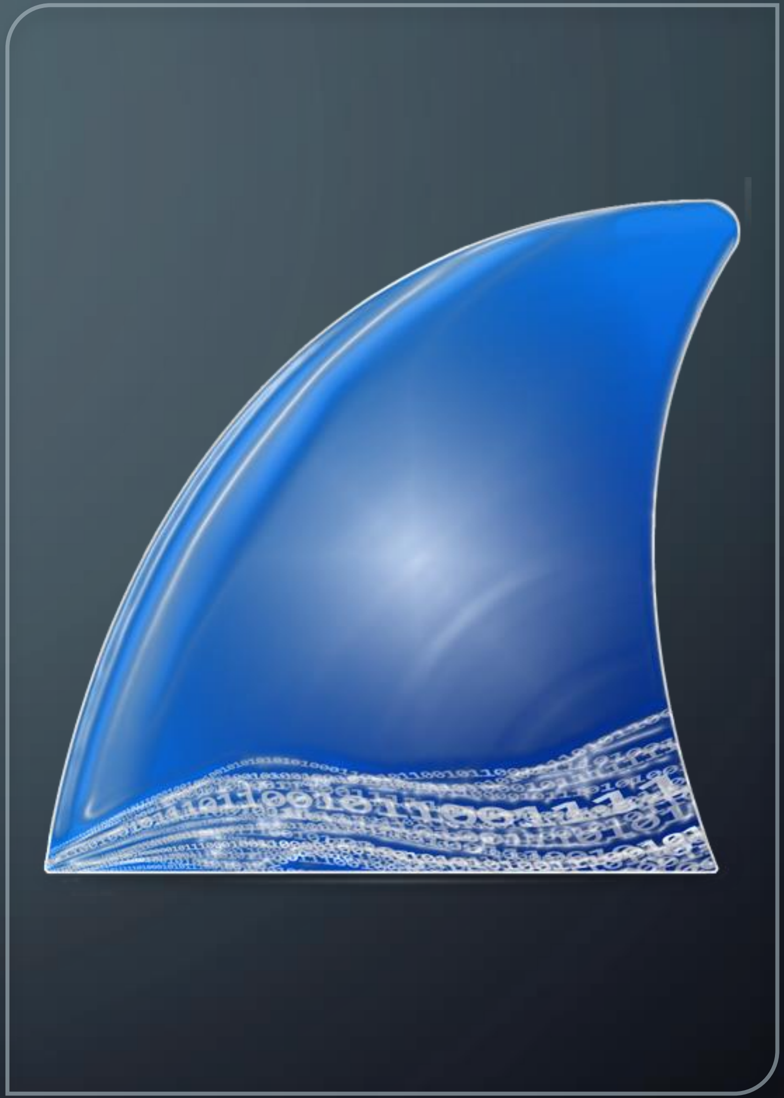
	Real-Time/ Near-Real-Time	Postcompromise (Days/Weeks)
Network	Network Traffic Analysis Style 1	Network Forensics Style 2
Payload	Payload Analysis Style 3	
Endpoint	Endpoint Behavior Analysis Style 4	Endpoint Forensics Style 5

WIRESHARK

Le premier outil à connaître pour l’analyse de trafic réseau.

Aussi très pertinents :

- **tshark** – CLI
- **pyshark** – module python (wrapper de tshark)



DANS LES CTFS

- (Généralement) moins dans l’IR, plus dans la recherche de données
- Challenge classique :
    1. Compréhension du/des **protocoles**
    2. Compréhension du **format** des données
    3. **Extraction** de l’information pertinente
    4. (Si applicable) **Traitement** de l’information pour retrouver le message (le FLAG)

CHALLENGES !

nsec

HF

MontréHack

SÉLECTION DE CHALLENGES DE CTFS

1. Autograph (NorthSec 2021) – Trafic USB (signature électronique)
2. Hellcorp (Hackfest 2021) – Trafic chiffré
3. Portobello 53 (NorthSec 2022) – Exfiltration (très longue track)
4. Flickering Light Bulb (Hackfest 2022) – IoT
5. Aquavenia (MontréHack – H0h0h0day 2022)

1. AUTOGRAPH

I have heard that you have successfully gotten access into the Goldsmiths' Guild. We'll now need to take that covert action to the next step. Good luck.

The lobby is a small chamber with a second locked door and a desk on its side.

You hear from the other side of the door: "**You need to sign the certificate**".

Upon inspection, you see a screen that the voice called the "certificate". You find a jack and you **plug your sniffer** on it before leaving the guild.

You obtain **Signatures Captures** and go analyze them.

1. AUTOGRAPH – FLAG #1

What are the **vendor** and the **product name** of the USB device?

Format: flag-usb_[vendor]_[product]

Vendor hint: do not add Ltd., inc., corp., etc

1. AUTOGRAPH – FLAG #2

Decode the device input.

2. HELLCORP – FLAG #1

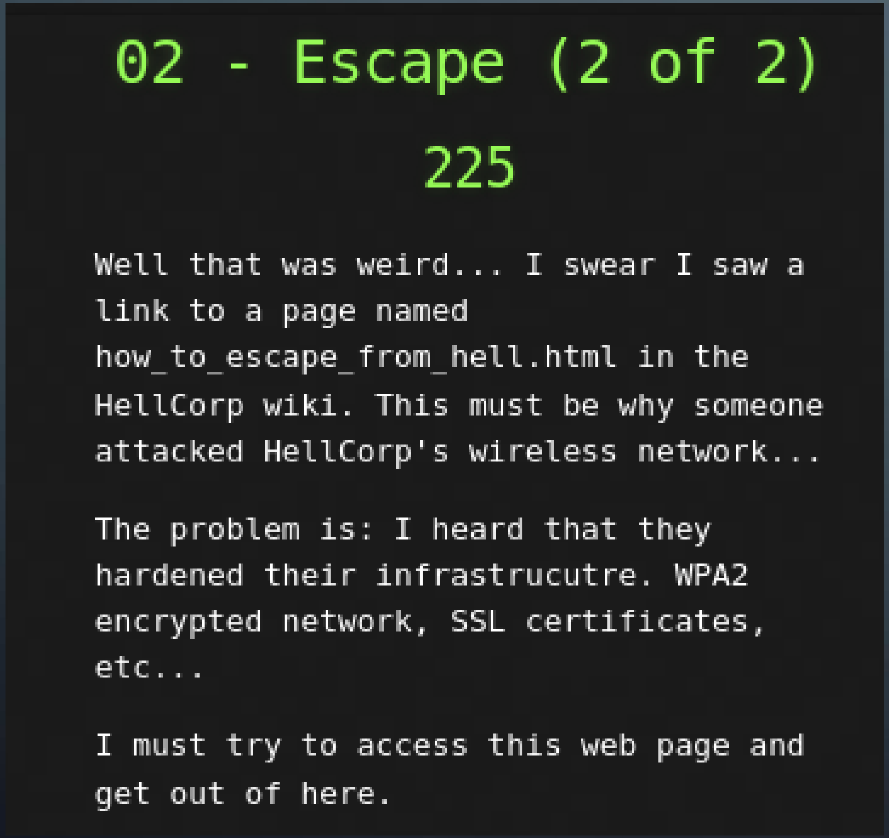
Pas réussi à retrouver la description…

Mais selon un write-up :

> “I did not get a screenshot of this challenge. But it was something about catching someone trying to escape from hell. We had a network capture of the Wi-Fi traffic to do it.”
>
> (https://erichogue.ca/2021/11/HackfestCTF/HellCorp)

Format du flag : HF-…

2. HELLCORP – FLAG #2



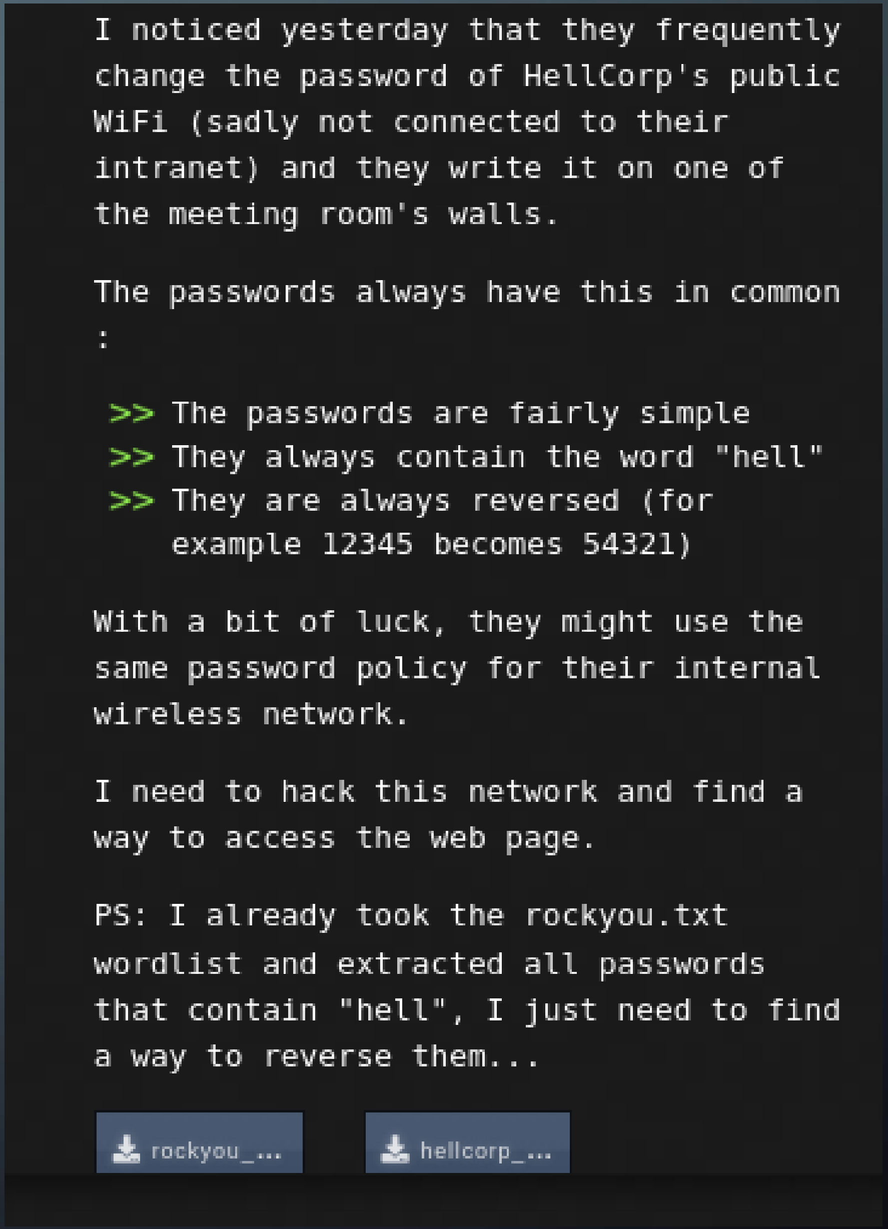
02 - Escape (2 of 2)

225

Well that was weird... I swear I saw a link to a page named how_to_escape_from_hell.html in the HellCorp wiki. This must be why someone attacked HellCorp's wireless network...

The problem is: I heard that they hardened their infrastrucutre. WPA2 encrypted network, SSL certificates, etc...

I must try to access this web page and get out of here.



I noticed yesterday that they frequently change the password of HellCorp's public WiFi (sadly not connected to their intranet) and they write it on one of the meeting room's walls.

The passwords always have this in common :

>> The passwords are fairly simple
>> They always contain the word "hell"
>> They are always reversed (for example 12345 becomes 54321)

With a bit of luck, they might use the same password policy for their internal wireless network.

I need to hack this network and find a way to access the web page.

PS: I already took the rockyou.txt wordlist and extracted all passwords that contain "hell", I just need to find a way to reverse them...

(https://erichogue.ca/2021/11/HackfestCTF/HellCorp)

3. PORTOBELLO 53 – DENIAL – FLAG #1

Any data leaving or entering the Mycoverse goes through our AI-backed deep packet inspection appliance. The vendor told us that this box was what we needed. At this price tag, I know he's right.

Why do you need **DNS logs** anyway? We both know that DNS servers are just address books of Internet resources and I've never seen anyone abuse a plain old address book.

The appliance would have blocked anything malicious anyway. I bet you don't even have a certification to **understand the protocol** anyway.

Here's a link to download the PCAP. Don't waste your time on the network capture, I skimmed throught it and found that your **test device fd00:6e73:6563:3232::beef** did nothing suspicious.

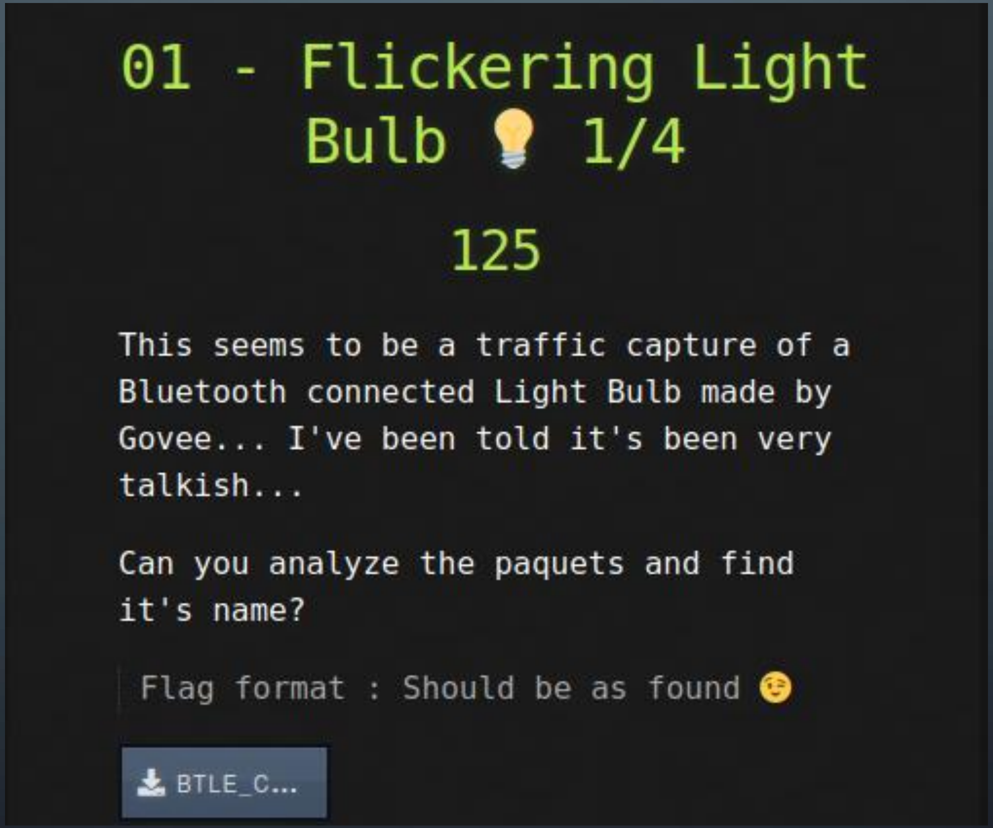
Rosie Meyer - A+, Server+, CCNA, CCNP, CCIE, MSDST, CSM

Network Admin

3. PORTOBELLO 53 – DENIAL – FLAG #2

I bet this is just a malformed DNS query. There's no way a server would answer to this.

4. FLICKERING LIGHT BULB – FLAG #1



01 - Flickering Light Bulb 💡 1/4

125

This seems to be a traffic capture of a Bluetooth connected Light Bulb made by Govee... I've been told it's been very talkish...

Can you analyze the paquets and find it's name?

> Flag format : Should be as found 😉

4. FLICKERING LIGHT BULB – FLAGS #2-4

Pas réussi à retrouver les descriptions, aucun write-up existant…

De mémoire il fallait interpréter les commandes envoyées au device et écrire des nouvelles commandes en fonction de ça.

Mais sans la description…

5. AQUAVENIA – FLAG #1

You work for Evien, a compagny that sells water bottles. Your main competitor, Aquaviena, has recently launched a new "life-flavoured" water bottle. This life flavour forever changed the water-bottle industry, made Aquaviena the king of the market and made Evien's sales tank. Nobody outside Aquaviena knows how this flavour works, but it gives people an temporary, unconditional will to live and be happy.

Recently, an Aquaviena employee sent Evien a pcap file that, according to the anonymous source, reveals the secret of the life-flavoured water. The packets would come from a **subnet in Aquaviena's internal network**. Analyse this packet capture file to unveil the secret of Aquaviena. Your first task consist in **identifying the plan of Aquaviena** in case they get sued regarding their life-flavoured water. Flag format --> FLAG-.+

5. AQUAVENIA – FLAG #2

The anonymous source said that the secret came from a **conversation between two employees**. Find their **username**. Flag format is name1name2.

5. AQUAVENIA – FLAG #3

Find the name of the **person who got the idea** for the life-flavoured water.

5. AQUAVENIA – FLAG #4

Find the **secret ingredient** for the life-flavoured water.

MERCI !