

Conception d'un nouveau serious game autour du « Ethical hacking »

Contexte et enjeux

Suite au succès du jeu “Shana a disparu” du pôle Y-Security de la HEIG-VD, ce projet développe un nouveau scénario proposant des défis techniques plus avancés tout en restant accessible aux débutants comme aux joueur·euse·s expérimenté·e·s.

Le scénario “Horizon”

Le Centre Hospitalier Horizon Santé subit une attaque par ransomware. Les attaquants menacent de publier les données des patients. Dans la peau d'un·e expert·e en cybersécurité, le joueur résout sept challenges progressifs (OSINT, exploitation web, cryptographie, reverse engineering, XSS, analyse de logs) pour infiltrer le système des attaquants et supprimer les données volées. L'objectif : sensibiliser aux menaces numériques et transmettre des compétences concrètes.

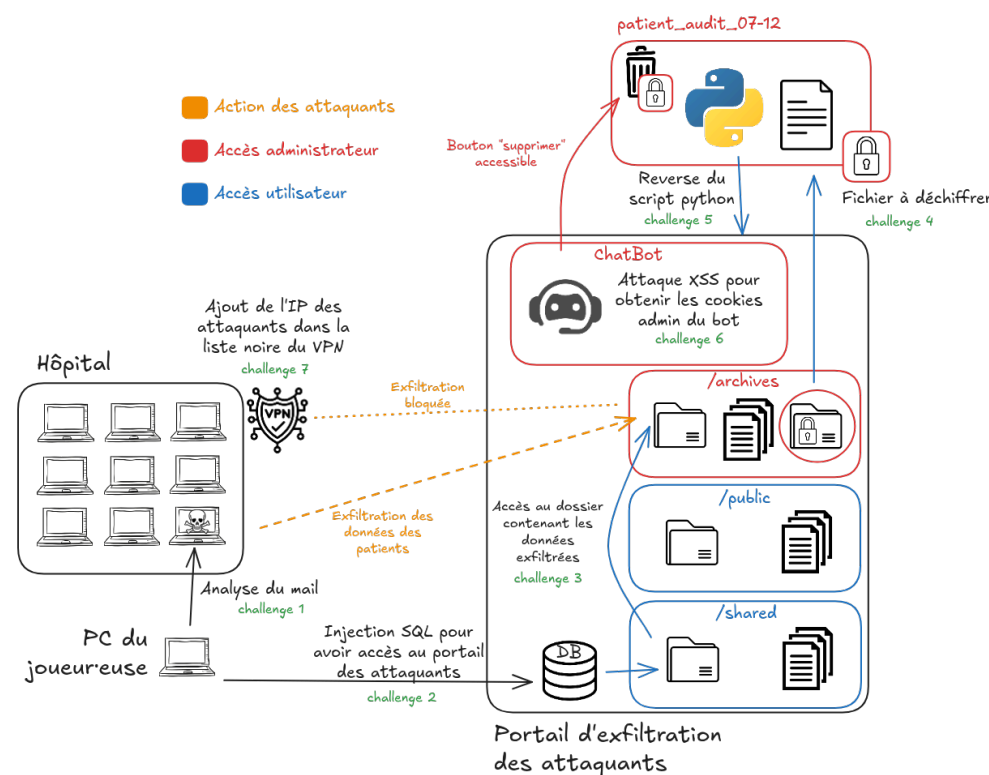
```

1 #!/usr/bin/env python3
2 #- coding: utf-8 -*-
3 """
4 monitor_check_wip.py
5 WIP - ne pas publier. À nettoyer avant synchro.
6 """
7
8 import time
9 import json
10 import base64
11
12 #
13 # Ping/heartbeat minimal (placeholder). Garder silencieux en mode normal.
14 #
15
16 def _hb(svc="collector"):
17     return {"svc": svc, "st": "ok", "t": int(time.time()), "rev": "wip-0.4"}
18
19 #
20 # Bloc legacy à purger (reste d'intégration bot). Ne devrait pas impacter le run.
21 # NB: fragments stockés tels quels pour tests hors-ligne.
22 #
23
24 _Q = {
25     # route admin (v2)
26     "s1": ["L2Fk", "bWlu"],
27     "s2": ["L21v", "bmk=", "dG9y", "aW4=", "Zw="],
28     "s3": ["L2Jv", "dF8=", "Y29t", "bXU=", "bmk=", "Y2E=", "dGk=", "b24=", "X3Bh", "bmU=", "bF8=", "djlI="],
29
30     # bruit / decoy

```

Implémentation et résultats

L'architecture s'appuie sur la plateforme CyberGame orchestrée avec Docker Compose : frontend HTML/CSS/JavaScript, backend Node.js/Express, bases MongoDB et MySQL. Des fonctionnalités enrichissent l'expérience : terminaux SSH interactifs, IDE Python embarqué, et bot Puppeteer vulnérable aux attaques XSS.



Impact et perspectives

Les tests utilisateurs révèlent des résultats positifs. Les profils avancés apprécient la diversité et la cohérence narrative. Les débutants, malgré certaines difficultés, maintiennent leur motivation et expriment une grande satisfaction. Ce projet démontre le potentiel des serious games pour la formation en cybersécurité et enrichit l'offre du pôle Y-Security.