Cyber Défense des infrastructures.

Module : Cyber Defense des infrastructures / EPITECH
Groupe : C'est down ou quoi ?
Type de document : Audit de la machine 10.10.10.7

On fait un nmap pour avoir les ports de la machine.

```
→  Bureau nmap 10.10.10.7

Starting Nmap 7.40 ( https://nmap.org ) at 2023-01-07 10:42 CET
Nmap scan report for 10.10.10.7
Host is up (0.062s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 3.53 seconds
```

Avec les flags on obtient plus de détails

$nmap -sS -v -v -Pn 10.10.10.7

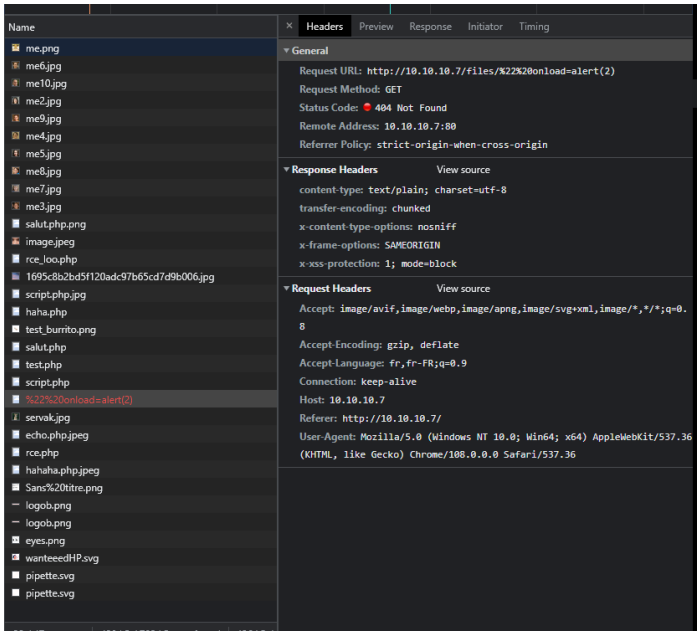
```
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63
```

On se rend sur le port 80 pour voir le site infecté, on se rend compte qu'on peut éventuellement faire des requêtes pour envoyer des fichiers. Peut-être que le malware est passé par ici, ou que c'est la conséquence.

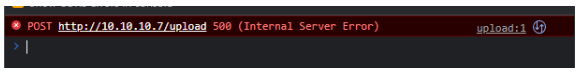
```
FileSystemException: Cannot open file, path = '/uploadedFiles/' (OS Error: Is a directory, errno = 21)
```

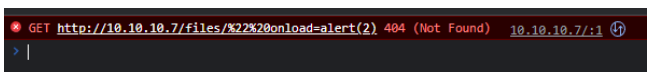
Je teste le system de push pour ajouter une image et cela fonctionne.

Il n'y a rien de suspicieux dans l'HTML



Il y a juste une image étrange qui pourrai être la source de notre problème.





Utilisation de Nikto pour scanner la machine infectée, dans une VM kali :

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nikto -h 10.10.10.7 -F txt -o scan.txt -useproxy

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.7
+ Target Hostname:    10.10.10.7
+ Target Port:        80
+ Start Time:         2023-01-07 05:36:47 (GMT-5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  11 error(s) and 1 item(s) reported on remote host
+ End Time:           2023-01-07 05:41:15 (GMT-5) (268 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
kali > Desktop > ≡ scan.txt
- Nikto v2.1.6/2.1.5
+ Target Host: 10.10.10.7
+ Target Port: 80
+ TCDAISEU Web Server returns a valid response with junk HTTP methods, this may cause false positives.
```

On ne trouve pas la bannière du site et il n'y a pas de CGI.

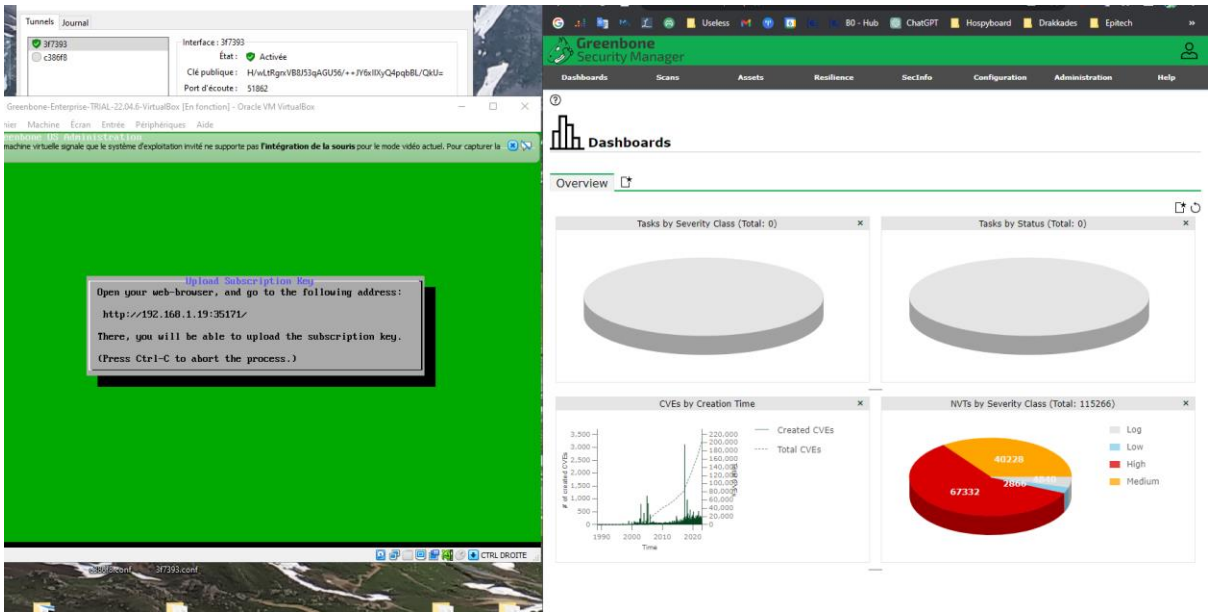
Et il soupçonne un faux positif sur la méthode http.

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 10.10.10.7 -p 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.7
+ Target Hostname:    10.10.10.7
+ Target Port:        80
+ Start Time:         2023-01-07 05:37:54 (GMT-5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  11 error(s) and 1 item(s) reported on remote host
+ End Time:           2023-01-07 05:42:21 (GMT-5) (267 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

J'ai aussi essayé en utilisant le port 80 comme cible principal et rien de plus.

Il est donc probable que le souci soit des faux positif au retour des requêtes http.

Essaye de greenbone



Et Nessus