Rapport de la première journée de Yday

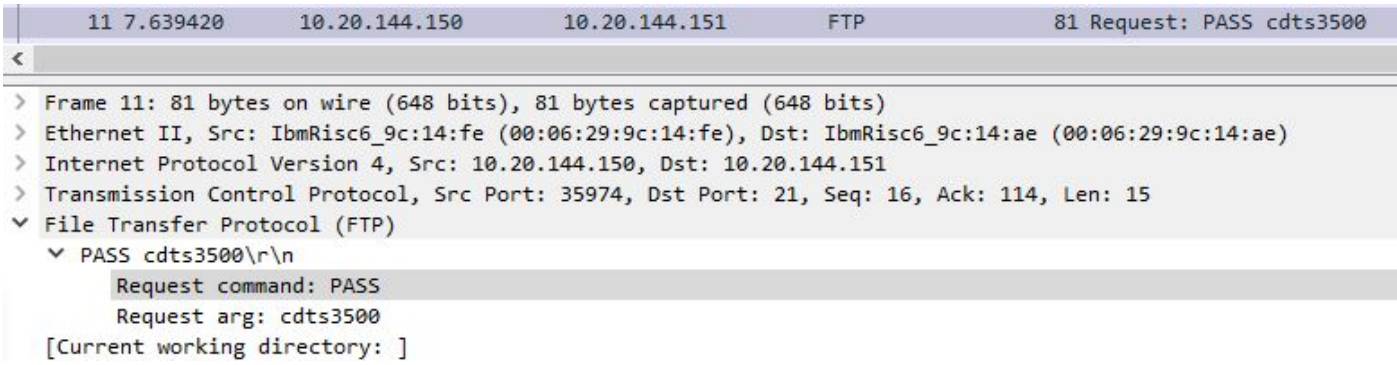
Sommaire des exercices réseaux:

18 Challenges

Résultats	Nom	Validations		Nombre de points	Difficulté
✔	FTP - Authentification	31%	59283	5	
✔	TELNET - authentification	27%	52267	5	
✔	ETHERNET - trame	21%	40662	10	
✔	Authentification twitter	24%	45999	15	
✔	Bluetooth - Fichier inconnu	6%	11581	15	
✔	CISCO - mot de passe	15%	29221	15	
✔	DNS - transfert de zone	8%	14056	15	
✔	IP - Time To Live	15%	27888	15	
✔	LDAP - null bind	5%	8172	15	
✔	SIP - Authentification	12%	23378	20	

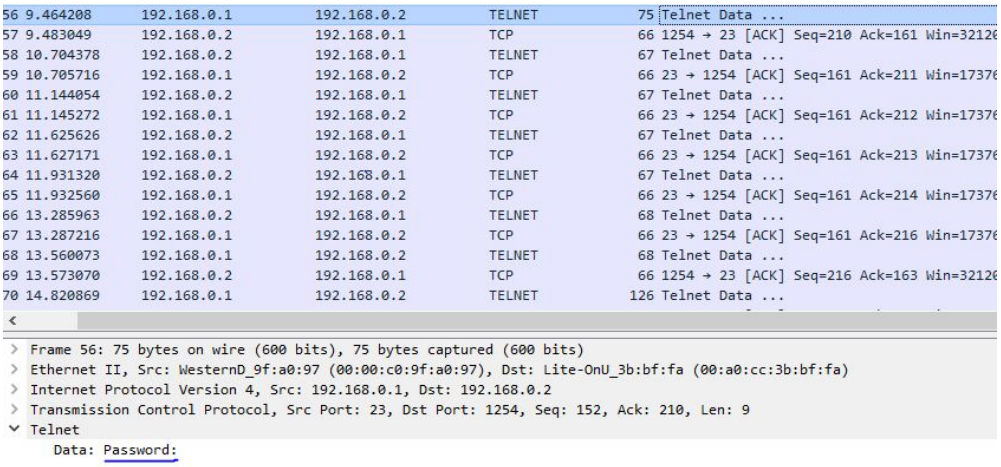
1)FTP - Authentification

Le mot de passe été donné dans le paquet 11 et j'étais clairement dis “cdts3500”.

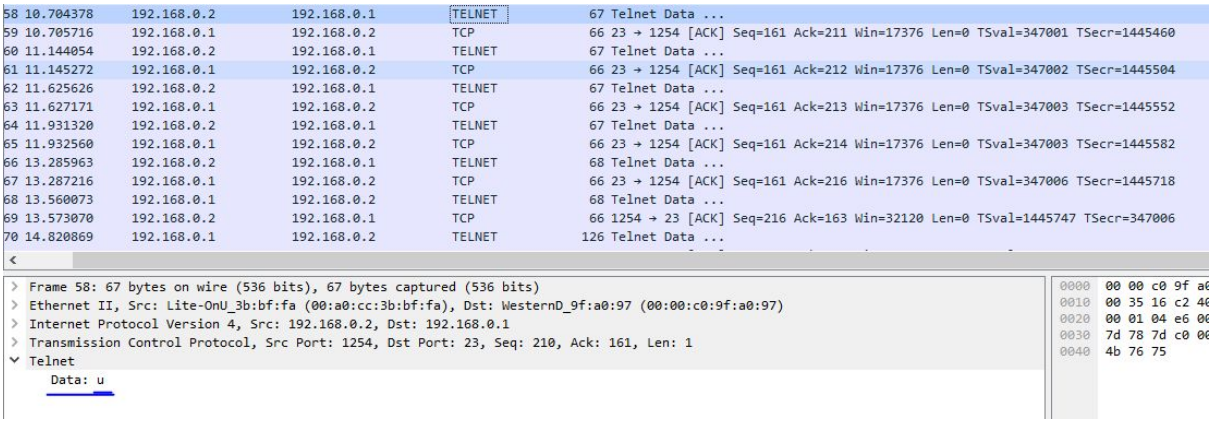


2)TeLNET - Authentification

Pour résoudre celui-ci : il fallait regardé la tranche Telnet et trouvé la frame ou le password était évoqué



Ensuite on marque toutes les lettres du password pour que ça nous donne : “user”

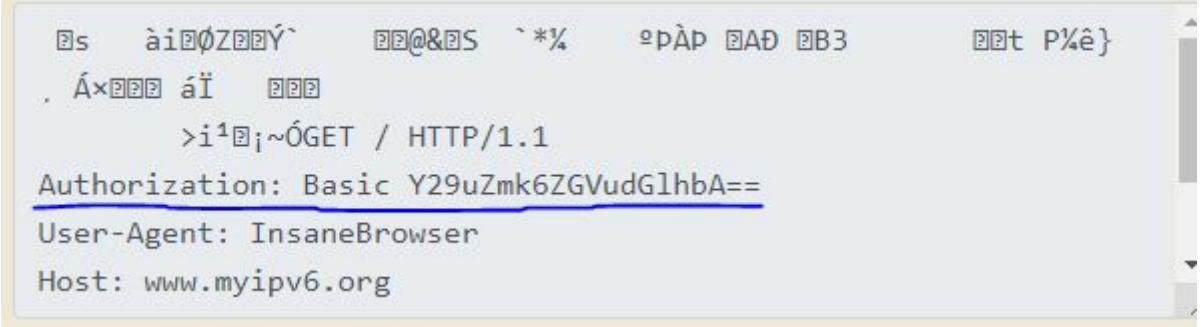


3)ETHERNET - trame

On nous donne cette trame :

```
00 05 73 a0 00 00 e0 69 95 d8 5a 13 86 dd 60 00
00 00 00 9b 06 40 26 07 53 00 00 60 2a bc 00 00
00 00 ba de c0 de 20 01 41 d0 00 02 42 33 00 00
00 00 00 00 00 04 96 74 00 50 bc ea 7d b8 00 c1
d7 03 80 18 00 e1 cf a0 00 00 01 01 08 0a 09 3e
69 b9 17 a1 7e d3 47 45 54 20 2f 20 48 54 54 50
2f 31 2e 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74
69 6f 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a
6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d
0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73
61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74
3a 20 77 77 77 2e 6d 79 69 70 76 36 2e 6f 72 67
0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d
0a
```

Pour trouver la réponse il faut prendre cette trame et la converti en Ascii ,ce qui nous donne ceci :

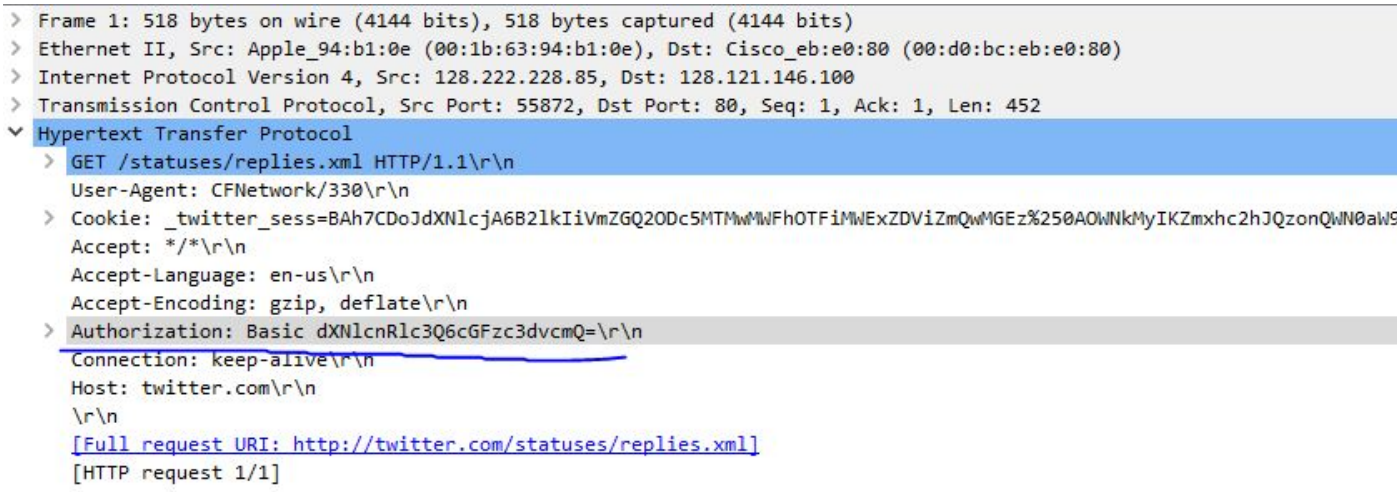


Après on converti “Y29uZmk6ZGVudGlhbA==” en Base64 ce qui nous donne le password “confi:dential”

4)Authentification twitter

Du coup , on fait comme celui haut dessus :

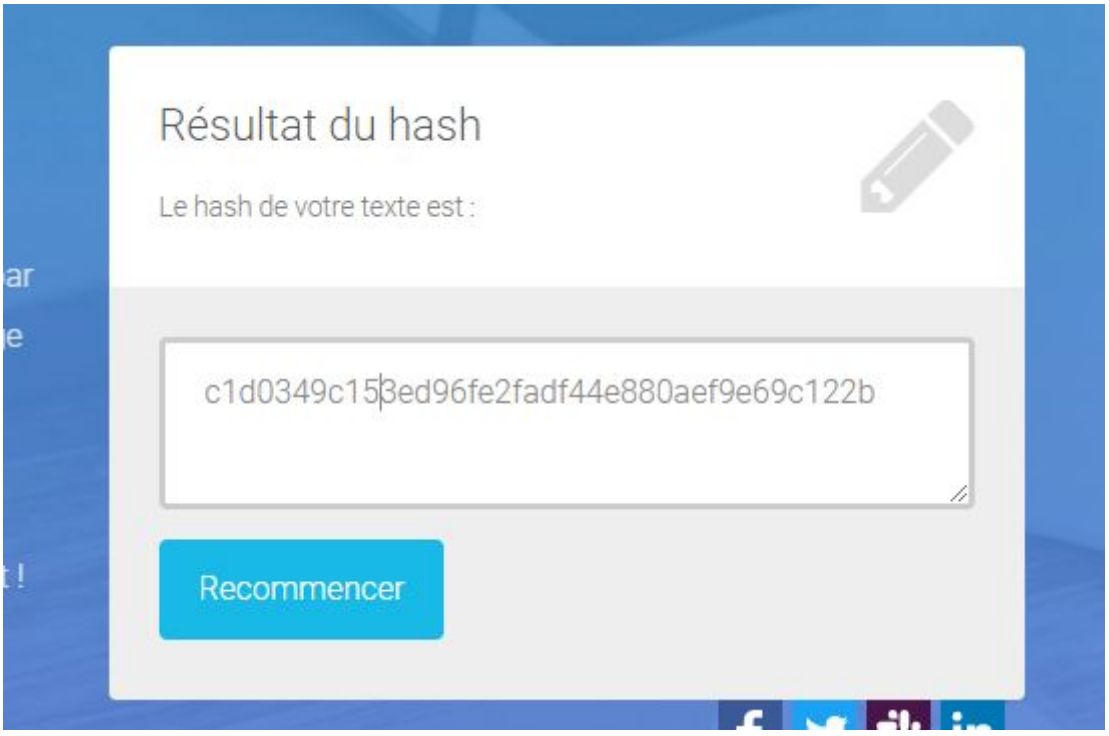
“**dXNlcnRlc3Q6cGFzc3dvcmQ=** “ nous donne en Base64 “**usertest:password**” du coup le password est “**password**”



5)Bluetooth - Fichier inconnu

```
Bluetooth HCI Event - Remote Name Request Complete
    Event Code: Remote Name Request Complete (0x07)
    Parameter Total Length: 255
    Status: Success (0x00)
    BD_ADDR: SamsungE_b9:4f:c6 (0c:b3:19:b9:4f:c6)
    Remote Name: GT-S7390G
```

Comme indiqué dans l'exercice j'ai cherché l'adresse MAC et le modèle du téléphone dans une trame.Puis j'ai converti en SHA1 l'adresse MAC et le modèle "0C:B3:19:B9:4F:C6GT-S7390G" et ca nous donne "c1d0349c153ed96fe2fadf44e880aef9e69c122b" en password



6)CISCO - mot de passe

Avec un décodeur CISCO on obtient ceci , du coup on en déduit que le password est “**6sK0_enable**”

HASH Cisco 7 demandé : 025017705b3907344e
Mot de passe correspondant : 6sK0_hub

HASH Cisco 7 demandé : 10181a325528130f010d24
Mot de passe correspondant : 6sK0_admin

HASH Cisco 7 demandé : 124f163c42340b112f3830
Mot de passe correspondant : 6sK0_guest

7)DNS - transfert de zone

Pour celui-ci , on lance la vm kali et on tape "dig @212.129.38.224 -p 54011 txt ch11.challenge01.root-me.org” dans le cmd ce qui nous donne ceci :

On comprend vite que le password est la secret key

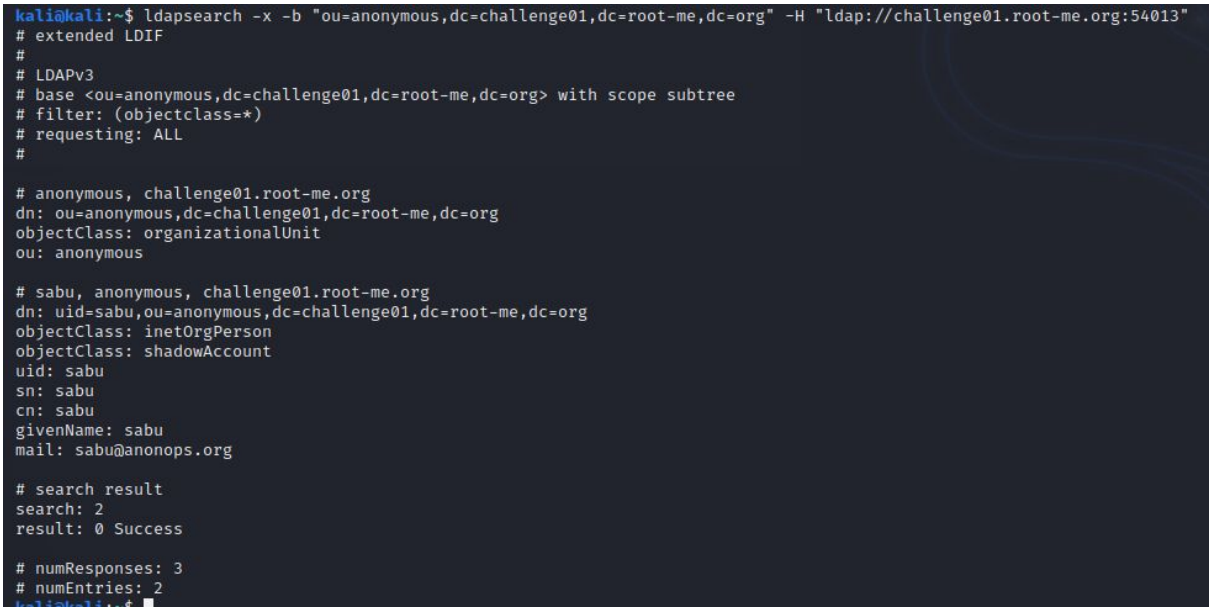
8)IP - Time To Live

```
106 Echo (ping) request  id=0x0200, seq=6144/24, ttl=8 (no response found!)
182 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=6400/25, ttl=8 (no response found!)
182 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=6656/26, ttl=8 (no response found!)
182 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=6912/27, ttl=9 (no response found!)
182 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=7168/28, ttl=9 (no response found!)
182 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=7424/29, ttl=9 (no response found!)
182 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=7680/30, ttl=10 (no response found!)
 70 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=7936/31, ttl=10 (no response found!)
 70 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=8192/32, ttl=10 (no response found!)
 70 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=8448/33, ttl=11 (no response found!)
 70 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=8704/34, ttl=11 (no response found!)
 70 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=8960/35, ttl=11 (no response found!)
 70 Time-to-live exceeded (Time to live exceeded in transit)
 70 Destination unreachable (Port unreachable)
106 Echo (ping) request  id=0x0200, seq=9216/36, ttl=12 (no response found!)
 70 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=9472/37, ttl=12 (no response found!)
 70 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=9728/38, ttl=12 (no response found!)
 70 Time-to-live exceeded (Time to live exceeded in transit)
106 Echo (ping) request  id=0x0200, seq=9984/39, ttl=13 (reply in 72)
106 Echo (ping) reply    id=0x0200, seq=9984/39, ttl=51 (request in 71)
106 Echo (ping) request  id=0x0200, seq=10240/40, ttl=13 (reply in 74)
106 Echo (ping) reply    id=0x0200, seq=10240/40, ttl=51 (request in 73)
```

En parcourant les trames, on voit que la conversation change radicalement à partir de TTL =13 alors qu'avant le serveur affichait que la requête expirait dans le transit.Donc on déduit que la réponse est 13.

9)LDAP - null bind

On recherche l'email des anonymous qui se sont installé dans l'annuaire LDAP. Du coup ,on relance la vm pour exécuter cette commande "**ldapsearch -x -b "ou=anonymous,dc=challenge01,dc=root-me,dc=org" -H "ldap://challenge01.root-me.org:54013"** "



On remarque que son email est donc "sabu@anonops.org"

10)SIP - Authentification

Dans cette exercice on nous donne ceci :

```
172.25.105.3"172.25.105.40"555"asterisk"REGISTER"sip:172.25.105.40"4787f7ce""""PLAIN"1234
172.25.105.3"172.25.105.40"555"asterisk"INVITE"sip:1000@172.25.105.40"70fbfdae""""MD5"aa533f6efa2b2abac675c1ee6cbde327
172.25.105.3"172.25.105.40"555"asterisk"BYE"sip:1000@172.25.105.40"70fbfdae""""MD5"0b306e9db1f819dd824acf3227b60e07
```

On peut voir que c'est 3 lignes commence par 2 IPS puis il vient register,invite,bye.On peut déduire que sur la ligne register ce que suit register est le login et que Plain est le mot de passe du coup "1234" est le mot de passe.