

Rapport de la première journée de Yday

Sommaire des exercices réseaux:

1. FTP - Authentification
2. TeLNET - Authentification
3. ETHERNET - trame
4. Authentification twitter
5. Bluetooth - Fichier inconnu
6. CISCO - mot de passe
7. DNS - transfert de zone
8. IP - Time To Live
9. LDAP - null bind
10. SIP - Authentification



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	19% 29221	15	
✓	DNS - transfert de zone	8% 14056	15	
✓	IP - Time To Live	19% 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".

11	7.639420	10.20.144.150	10.20.144.151	FTP	81 Request: PASS cdts3500
<					
> Frame 11: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)					
> Ethernet II, Src: IbmRisc6_9c:14:fe (00:06:29:9c:14:fe), Dst: IbmRisc6_9c:14:ae (00:06:29:9c:14:ae)					
> Internet Protocol Version 4, Src: 10.20.144.150, Dst: 10.20.144.151					
> Transmission Control Protocol, Src Port: 35974, Dst Port: 21, Seq: 16, Ack: 114, Len: 15					
▼ File Transfer Protocol (FTP)					
▼ PASS cdts3500\r\n					
Request command: PASS					
Request arg: cdts3500					
[Current working directory:]					

2)TelNET - Authentification

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

56	9.464208	192.168.0.1	192.168.0.2	TELNET	75 Telnet Data ...
57	9.483049	192.168.0.2	192.168.0.1	TCP	66 1254 → 23 [ACK] Seq=210 Ack=161 Win=32126
58	10.704378	192.168.0.2	192.168.0.1	TELNET	67 Telnet Data ...
59	10.705716	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=211 Win=17376
60	11.144054	192.168.0.2	192.168.0.1	TELNET	67 Telnet Data ...
61	11.145272	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=212 Win=17376
62	11.625626	192.168.0.2	192.168.0.1	TELNET	67 Telnet Data ...
63	11.627171	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=213 Win=17376
64	11.931320	192.168.0.2	192.168.0.1	TELNET	67 Telnet Data ...
65	11.932560	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=214 Win=17376
66	13.285963	192.168.0.2	192.168.0.1	TELNET	68 Telnet Data ...
67	13.287216	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=216 Win=17376
68	13.560073	192.168.0.1	192.168.0.2	TELNET	68 Telnet Data ...
69	13.573070	192.168.0.2	192.168.0.1	TCP	66 1254 → 23 [ACK] Seq=216 Ack=163 Win=32126
70	14.820869	192.168.0.1	192.168.0.2	TELNET	126 Telnet Data ...
<					
> Frame 56: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)					
> Ethernet II, Src: WesternD_9f:a0:97 (00:00:c0:9f:a0:97), Dst: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa)					
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2					
> Transmission Control Protocol, Src Port: 23, Dst Port: 1254, Seq: 152, Ack: 210, Len: 9					
▼ Telnet					
Data: Password:					

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

58	10.704378	192.168.0.2	192.168.0.1	TELNET	67 Telnet Data ...
59	10.705716	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=211 Win=17376 Len=0 TSval=347001 TSecr=1445460
60	11.144054	192.168.0.2	192.168.0.1	TELNET	67 Telnet Data ...
61	11.145272	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=212 Win=17376 Len=0 TSval=347002 TSecr=1445504
62	11.625626	192.168.0.2	192.168.0.1	TELNET	67 Telnet Data ...
63	11.627171	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=213 Win=17376 Len=0 TSval=347003 TSecr=1445552
64	11.931320	192.168.0.2	192.168.0.1	TELNET	67 Telnet Data ...
65	11.932560	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=214 Win=17376 Len=0 TSval=347003 TSecr=1445582
66	13.285963	192.168.0.2	192.168.0.1	TELNET	68 Telnet Data ...
67	13.287216	192.168.0.1	192.168.0.2	TCP	66 23 → 1254 [ACK] Seq=161 Ack=216 Win=17376 Len=0 TSval=347006 TSecr=1445718
68	13.560073	192.168.0.1	192.168.0.2	TELNET	68 Telnet Data ...
69	13.573070	192.168.0.2	192.168.0.1	TCP	66 1254 → 23 [ACK] Seq=216 Ack=163 Win=32120 Len=0 TSval=1445747 TSecr=347006
70	14.820869	192.168.0.1	192.168.0.2	TELNET	126 Telnet Data ...

> Frame 58: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)

> Ethernet II, Src: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD_9f:a0:97 (00:00:c0:9f:a0:97)

> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1

> Transmission Control Protocol, Src Port: 1254, Dst Port: 23, Seq: 210, Ack: 161, Len: 1

▼ Telnet

 Data: u

```

0000 00 00 c0 9f a0
0010 00 35 16 c2 46
0020 00 01 04 e6 06
0030 7d 78 7d c0 06
0040 4b 76 75

```

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 :

```

Es ài00Z00Y` 00Q&0S `*% 0pÀp 0A0 0B3 00t P%ê}
. Áx000 aİ 000
>i10;~0GET / HTTP/1.1
Authorization: Basic Y29uZmk6ZGVudGlhbA==
User-Agent: InsaneBrowser
Host: www.myipv6.org

```

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

4)Authentication twitter

Du coup , on fait comme celui haut dessus :

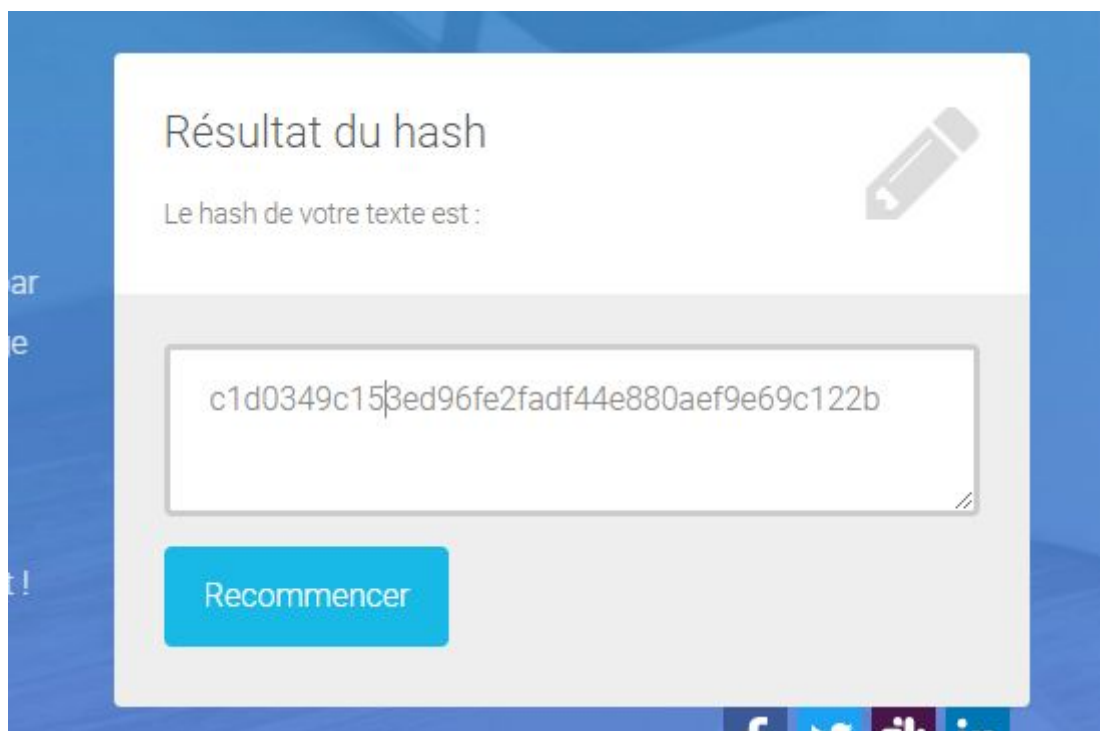
“dXNlcnRlc3Q6cGFzc3dvcmQ= ” nous donne en Base64 “usertest:password”
du coup le password est “password”

```
> Frame 1: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits)
> Ethernet II, Src: Apple_94:b1:0e (00:1b:63:94:b1:0e), Dst: Cisco_eb:e0:80 (00:d0:bc:eb:e0:80)
> Internet Protocol Version 4, Src: 128.222.228.85, Dst: 128.121.146.100
> Transmission Control Protocol, Src Port: 55872, Dst Port: 80, Seq: 1, Ack: 1, Len: 452
▼ Hypertext Transfer Protocol
  > GET /statuses/replies.xml HTTP/1.1\r\n
    User-Agent: CFNetwork/330\r\n
  > Cookie: _twitter_sess=BAh7CDoJdXNlcjA6B2lkIiVmZGQ2ODc5MTMwMWFhOTFiMWEExZDVhZmQwMGEz%250AOWNkMyIKZmxhc2hJQzonQWN0aW90\r\n
    Accept: */*\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
  > Authorization: Basic dXNlcnRlc3Q6cGFzc3dvcmQ=\r\n
    Connection: keep-alive\r\n
    Host: twitter.com\r\n
    \r\n
    [Full request URI: http://twitter.com/statuses/replies.xml]
    [HTTP request 1/1]
```

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 ça 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 :

```
kali@kali:~$ dig @212.129.38.224 -p 54011 txt ch11.challenge01.root-me.org

; <<>> DiG 9.16.4-Debian <<>> @212.129.38.224 -p 54011 txt ch11.challenge01.root-me.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 23957
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ch11.challenge01.root-me.org. IN      TXT

;; ANSWER SECTION:
ch11.challenge01.root-me.org. 604800 IN TXT      "DNS transfer secret key : CBkFRwfNMMtRjHY"

;; AUTHORITY SECTION:
ch11.challenge01.root-me.org. 604800 IN NS       ch11.challenge01.root-me.org.

;; ADDITIONAL SECTION:
ch11.challenge01.root-me.org. 604800 IN A         127.0.0.1

;; Query time: 16 msec
;; SERVER: 212.129.38.224#54011(212.129.38.224)
;; WHEN: Thu Oct 22 13:05:23 EDT 2020
;; MSG SIZE rcvd: 141
```

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" "

```
kali@kali:~$ ldapsearch -x -b "ou=anonymous,dc=challenge01,dc=root-me,dc=org" -H "ldap://challenge01.root-me.org:54013"
# extended LDIF
#
# LDAPv3
# base <ou=anonymous,dc=challenge01,dc=root-me,dc=org> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# anonymous, challenge01.root-me.org
dn: ou=anonymous,dc=challenge01,dc=root-me,dc=org
objectClass: organizationalUnit
ou: anonymous
# sabu, anonymous, challenge01.root-me.org
dn: uid=sabu,ou=anonymous,dc=challenge01,dc=root-me,dc=org
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: sabu
sn: sabu
cn: sabu
givenName: sabu
mail: sabu@anonops.org
# search result
search: 2
result: 0 Success
# numResponses: 3
# numEntries: 2
```

On remarque que son email est donc ["sabu@anonops.org"](mailto:sabu@anonops.org)

10)SIP - Authentication

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"70fbfdac""MD5"aa533f6efa2b2abac675c1ee6cbde327
172.25.105.3"172.25.105.40"555"asterisk"BYE"sip:1000@172.25.105.40"70fbfdac""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.