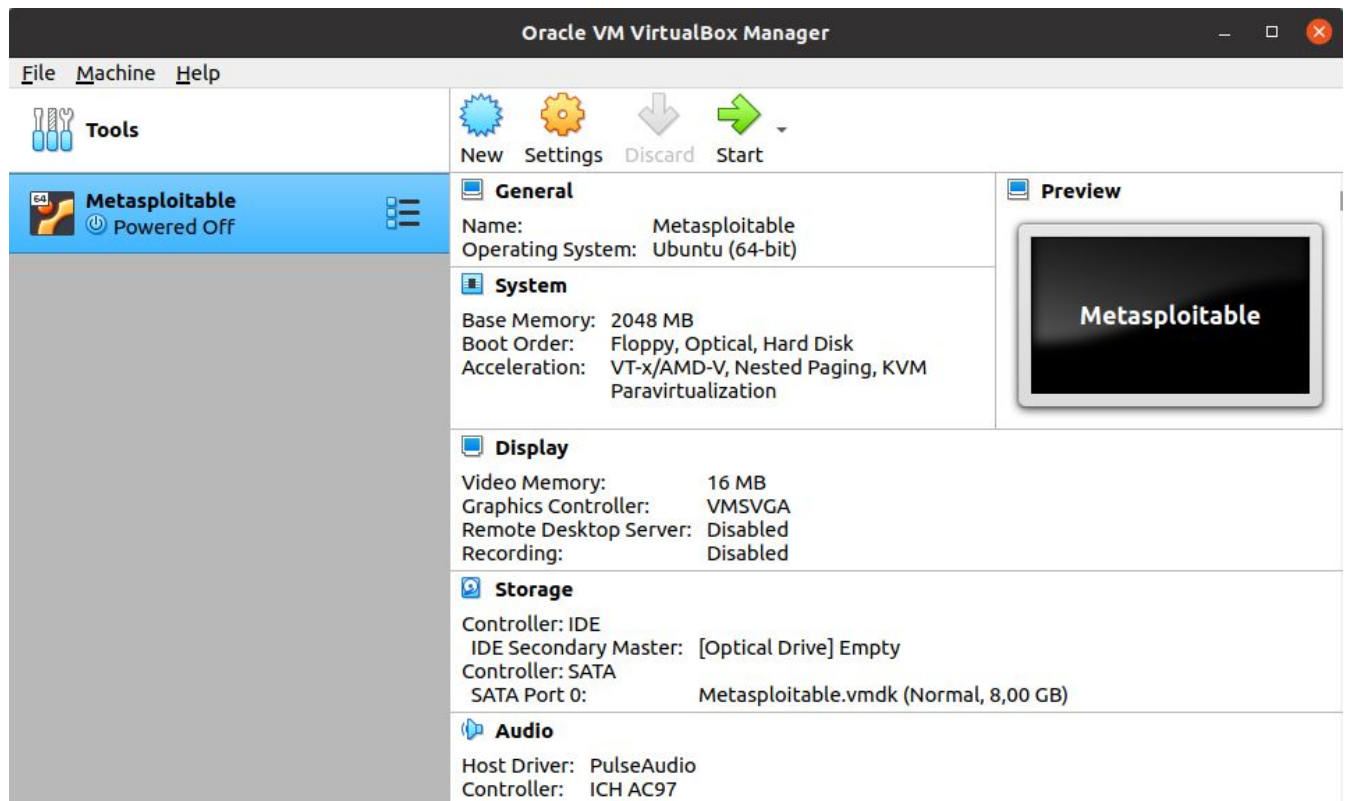


YDays - Séance 1

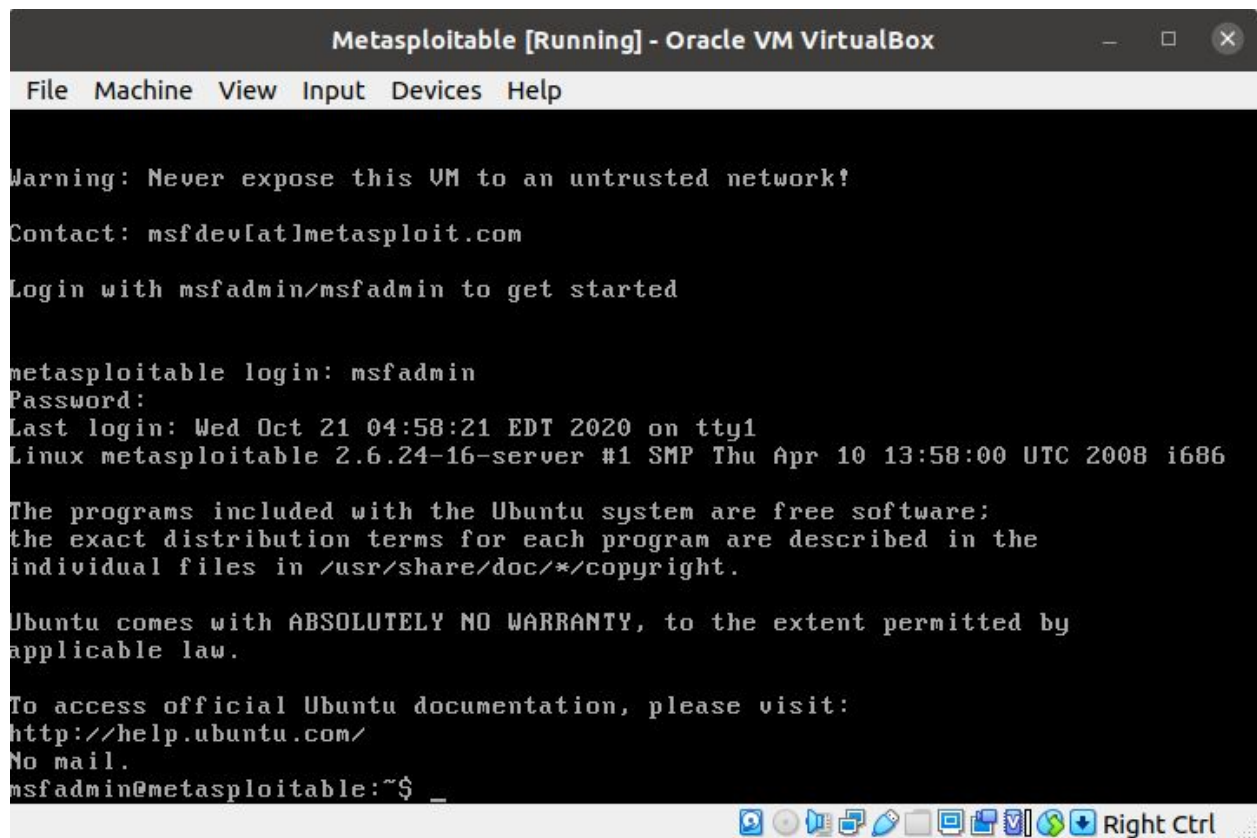
Installation de VirtualBox / Metasploitable

Dans un premier temps, j'ai installé VirtualBox. J'ai ensuite créé une instance de type Linux - Ubuntu 64 bits (voir image ci-dessus).

Puis, j'ai défini comme contrôleur SATA le fichier "*Metasploitable.vmdk*", de type *Virtual Machine Disk Format*, qui contient les fichiers du noyau du système d'exploitation, les pilotes de périphérique, les composants d'application et les fichiers de données qui vont permettre à la machine de fonctionner.



J'ai ensuite démarré la machine virtuelle, et je me suis connecté grâce aux identifiants *msfadmin:msfadmin*, comme indiqué dans la console de la machine virtuelle lors de son démarrage (voir image ci-dessous).



```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Wed Oct 21 04:58:21 EDT 2020 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

Console de connexion à la machine virtuelle

Pénétration réseau sur [Root-Me.org](https://root-me.org)

Avec des membres de mon groupe, nous sommes allé sur le site root-me.org afin de nous familiariser avec la pénétration réseau.

Les premiers exercices étaient plutôt simples, il fallait seulement analyser les trames afin de trouver le mot de passe (voir image ci-dessous).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.20.144.150	10.20.144.151	TCP	74	35974 → 21 [SYN] Seq=0 Win=32648 Len=0 MSS=1380 WS=1 TSval=1657560000 TS...
2	0.000320	10.20.144.151	10.20.144.150	TCP	78	21 → 35974 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1356 WS=1 TSval=16...
3	0.000570	10.20.144.150	10.20.144.151	TCP	66	35974 → 21 [ACK] Seq=1 Ack=1 Win=32648 Len=0 TSval=1657560000 TSecr=1657...
4	0.000630	10.20.144.151	10.20.144.150	FTP	106	Response: 220-QTCP at fran.csg.stercomm.com.
5	0.275440	10.20.144.150	10.20.144.151	TCP	66	35974 → 21 [ACK] Seq=1 Ack=37 Win=32648 Len=0 TSval=1657560500 TSecr=165...
6	0.275760	10.20.144.151	10.20.144.150	FTP	126	Response: 220 Connection will close if idle more than 5 minutes.
7	0.276140	10.20.144.150	10.20.144.151	TCP	66	35974 → 21 [ACK] Seq=1 Ack=93 Win=32648 Len=0 TSval=1657560500 TSecr=165...
8	4.216600	10.20.144.150	10.20.144.151	FTP	81	Request: USER cdts3500
9	4.217350	10.20.144.151	10.20.144.150	FTP	91	Response: 331 Enter password.
10	4.217630	10.20.144.150	10.20.144.151	TCP	66	35974 → 21 [PSH, ACK] Seq=16 Ack=114 Win=32648 Len=0 TSval=1657564500 TS...
11	7.639420	10.20.144.150	10.20.144.151	FTP	81	Request: PASS cdts3500
12	7.843260	10.20.144.151	10.20.144.150	TCP	70	21 → 35974 [PSH, ACK] Seq=114 Ack=31 Win=16384 Len=0 TSval=1657397500 TS...
13	8.184000	10.20.144.151	10.20.144.150	FTP	95	Response: 230 CDTs3500 logged on.
14	8.184360	10.20.144.150	10.20.144.151	TCP	66	35974 → 21 [PSH, ACK] Seq=31 Ack=139 Win=32648 Len=0 TSval=1657568500 TS...
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:]						
0000	00 06 29 9c 14 ae 00 06	29 9c 14 fe 08 00 45 00)			
0010	00 43 2d 76 40 00 40 06	d7 e9 0a 14 90 96 0a 14	.C-v@.@.			
0020	90 97 8c 86 00 15 01 c1	b9 c6 60 b5 3f 16 80 18 ?			
0030	7f 88 bb 15 00 00 01 01	08 0a 62 cc 7b 00 62 c9 b { b .			
0040	d3 50 50 41 53 53 20 63	64 74 73 33 35 30 30 0d	.PPASS c dts3500			
0050	0a		.			

Trame de paquets dans WireShark

Pour plusieurs autres exercices, il nous a fallu faire des conversions avec par exemple du hachage Cisco, en Base64 ou encore en SHA-1:

"String" en alphabet latin	Hash en SHA-1
<i>AB:CD:EF:12:34:56myPhone</i>	<i>023cc433c380c2618ed961000a681f1d4c44f8f1</i>
<i>0C:B3:19:B9:4F:C6GT-S7390G</i>	<i>c1d0349c153ed96fe2fADF44e880aef9e69c122b</i>

Par la suite, nous avons dû utiliser des commandes Unix pour par exemple accéder aux informations sur un nom de domaine ou une adresse IP:

- Commande dig, pour interroger des serveurs DNS:

```
≥ dig @212.129.38.224 -p 54011 txt ch11.challenge01.root-me.org
```

```
; <<>> DiG 9.16.1-Ubuntu <<>> @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: 36623

;; 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: 39 msec

;; SERVER: 212.129.38.224#54011(212.129.38.224)

;; WHEN: jeu. oct. 22 10:08:35 CEST 2020

;; MSG SIZE  rcvd: 141
```

-
- Commande ldapsearch, pour effectuer une recherche sur un serveur LDAP (*Lightweight Directory Access Protocol*):

```
≥ 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
```

En tout nous avons effectué une douzaine d'exercices, les suivants étant nettement plus compliqués.

Results	Name	Validations	
✓	FTP - authentication	31%	59283
✓	TELNET - authentication	27%	52267
✓	ETHERNET - frame	21%	40662
✓	Twitter authentication	24%	45999
✓	Bluetooth - Unknown file	5%	11581
✓	CISCO - password	13%	29221
✓	DNS - zone transfert	8%	14056
✓	IP - Time To Live	13%	27888
✓	LDAP - null bind	5%	8172
✓	SIP - authentication	12%	23378
✓	ETHERNET - Patched transmission	4%	7721
✓	Global System Traffic for Mobile communication	3%	3970
✗	SSL - HTTP exchange	2%	3862
✗	Netfilter - common mistakes	1%	1848
✗	SNMP - Authentification	1%	1826
✗	Wired Equivalent Privacy	1%	898
✗	ICMP payload	2%	3213
✗	XMPP - authentication	1%	1313

C'est ainsi que s'est achevée cette journée de projet YDays.