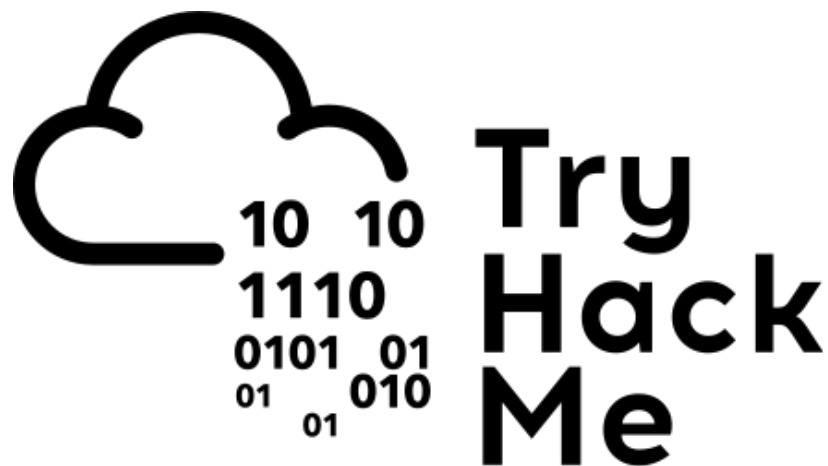


# YDays - Séance 3

Delbende Thomas

02/12/2020



## CTF sur [Root-Me.org](https://root-me.org)

Nous avons commencé cette nouvelle journée de YDays par un *Capture The Flag* sur le site root-me. Nous avons alors choisi la machine Metasploitable 2.



Salle 21 : Rejoindre la partie

Choisissez l'environnement virtuel que vous souhaitez attaquer

Metasploitable 2

Description

La deuxième machine virtuelle metasploitable fournie par Offensive Security.

Durée de la partie

60 min.

Soumettez votre vote

Enregistrer

Démarrer la partie

Démarrer la partie

L'environnement est en train de démarrer, soyez patient :)

### Informations

- Environnement virtuel choisi : **Metasploitable 2**
- Description :  
La deuxième machine virtuelle metasploitable fournie par Offensive Security. Durée de la partie : 60 min
- Le flag de validation est stocké dans le fichier **/passwd**
- Seules les personnes enregistrées pour cette partie peuvent attaquer cet environnement virtuel.
- Une temporisation empêche la partie de démarrer trop tôt ou trop tard.
- La partie démarrera lorsqu'un joueur (au minimum) aura choisi un environnement virtuel et se sera déclaré prêt.

Le but de cet exercice était de trouver un “flag” dans la machine mise à notre disposition, à l’emplacement */passwd*. Nous avons donc essayé d’y accéder grâce à un exécuteur de commande, qui exécutait pour nous des requêtes de type “ping”.

Cependant, il était possible de procéder à une “injection de commande”, en ajoutant à la suite de l’adresse à ping une autre commande:

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=0.000 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=0.000 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=0.000 ms  
  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2000ms  
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000 ms  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
passwd  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz
```

---

Nous pouvons effectivement voir sur l'image ci-dessus le fichier *passwd*, dont nous devons lire le contenu. Malheureusement, ce fichier était protégé par des droits de lecture restreints. Nous n'avons donc pas réussi à récupérer le "flag" à temps.

## Nmap sur [TryHackMe.com](https://tryhackme.com)

Nous sommes ensuite passés sur le site [tryhackme.org](https://tryhackme.org), où nous avons appris à utiliser la commande *nmap*, avec l'aide de Hellblade.

Perform some basic nmap scanning and learn to read through the results

---

Let's go ahead and start with the basics and perform a syn scan on the box provided. What will this command be without the host IP address?

Correct Answer

After scanning this, how many ports do we find open under 1000?

Correct Answer

What communication protocol is given for these ports following the port number?

Correct Answer

Hint

Perform a service version detection scan, what is the version of the software running on port 22?

Correct Answer

Hint

Perform an aggressive scan, what flag isn't set under the results for port 80?

Correct Answer

Hint

Perform a script scan of vulnerabilities associated with this box, what denial of service (DOS) attack is this box susceptible to? Answer with the name for the vulnerability that is given as the section title in the scan output. A vuln scan can take a while to complete. In case you get stuck, the answer for this question has been provided in the hint, however, it's good to still run this scan and get used to using it as it can be invaluable.

Correct Answer

Hint

Cet exercice de questionnaire nous a permis de nous familiariser avec l'utilisation de cette commande ainsi que les arguments qu'elle peut prendre, comme nous pouvons le voir sur l'image ci-dessous.

---

First, how do you access the help menu?

-h

Correct Answer

💡 Hint

Often referred to as a stealth scan, what is the first switch listed for a 'Syn Scan'?

-sS

Correct Answer

Not quite as useful but how about a 'UDP Scan'?

-sU

Correct Answer

What about operating system detection?

-O

Correct Answer

How about service version detection?

-sV

Correct Answer

Most people like to see some output to know that their scan is actually doing things, what is the verbosity flag?

-v

Correct Answer

What about 'very verbose'? (A personal favorite)

-vv

Correct Answer

Sometimes saving output in a common document format can be really handy for reporting, how do we save output in xml format?

-oX

Correct Answer

Aggressive scans can be nice when other scans just aren't getting the output that you want and you really don't care how 'loud' you are, what is the switch for enabling this?

-A

Correct Answer

💡 Hint

How do I set the timing to the max level, sometimes called 'Insane'?

-T5

Correct Answer

What about if I want to scan a specific port?

-p

Correct Answer

How about if I want to scan every port?

-p-

Correct Answer

What if I want to enable using a script from the nmap scripting engine? For this, just include the first part of the switch without the specification of what script to run.

--script

Correct Answer

What if I want to run all scripts out of the vulnerability category?

--script vuln

Correct Answer

💡 Hint

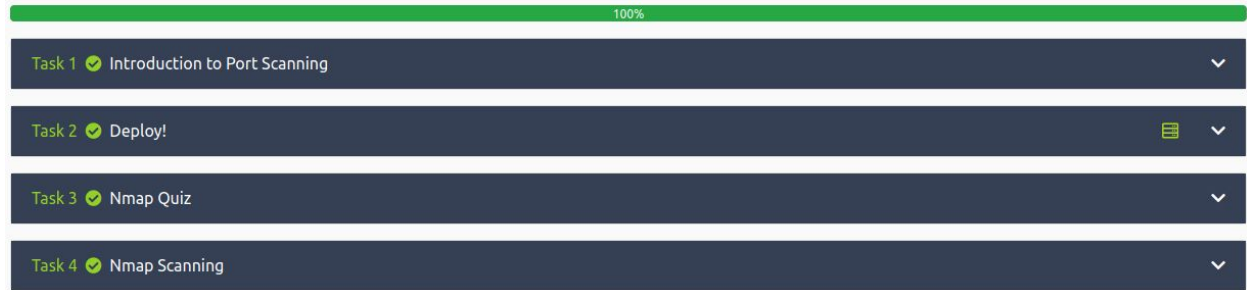
What switch should I include if I don't want to ping the host?

-Pn

Correct Answer

---

Nous avons cette fois réussi à répondre à toutes les questions dans les temps.



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