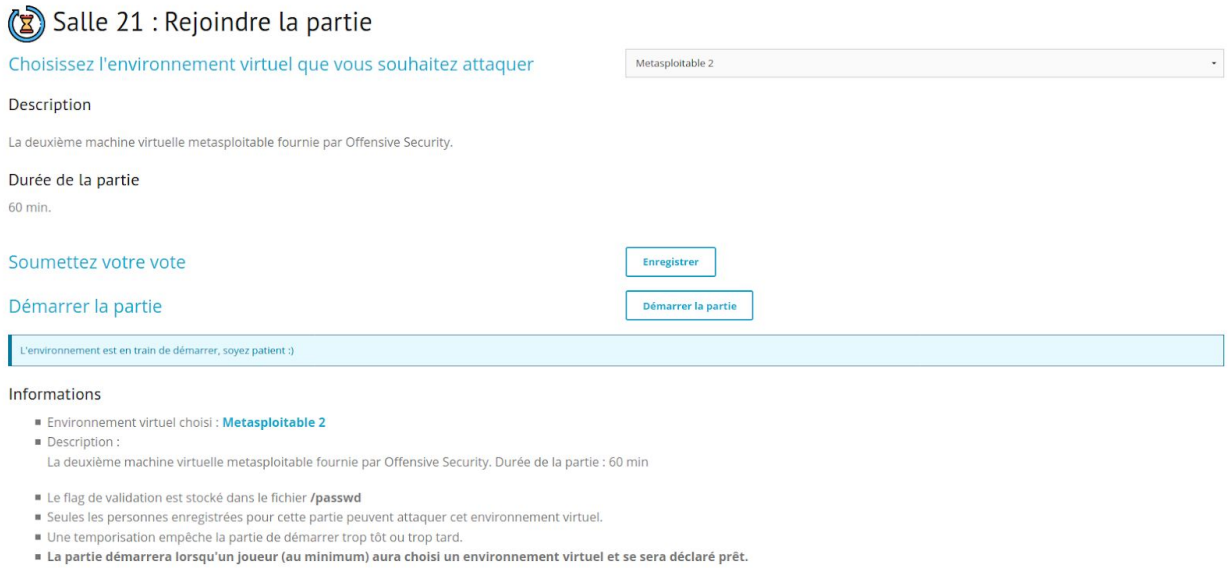
Projet ISO-03

YDays - Séance 3

Delbende Thomas 02/12/2020

CTF sur 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.



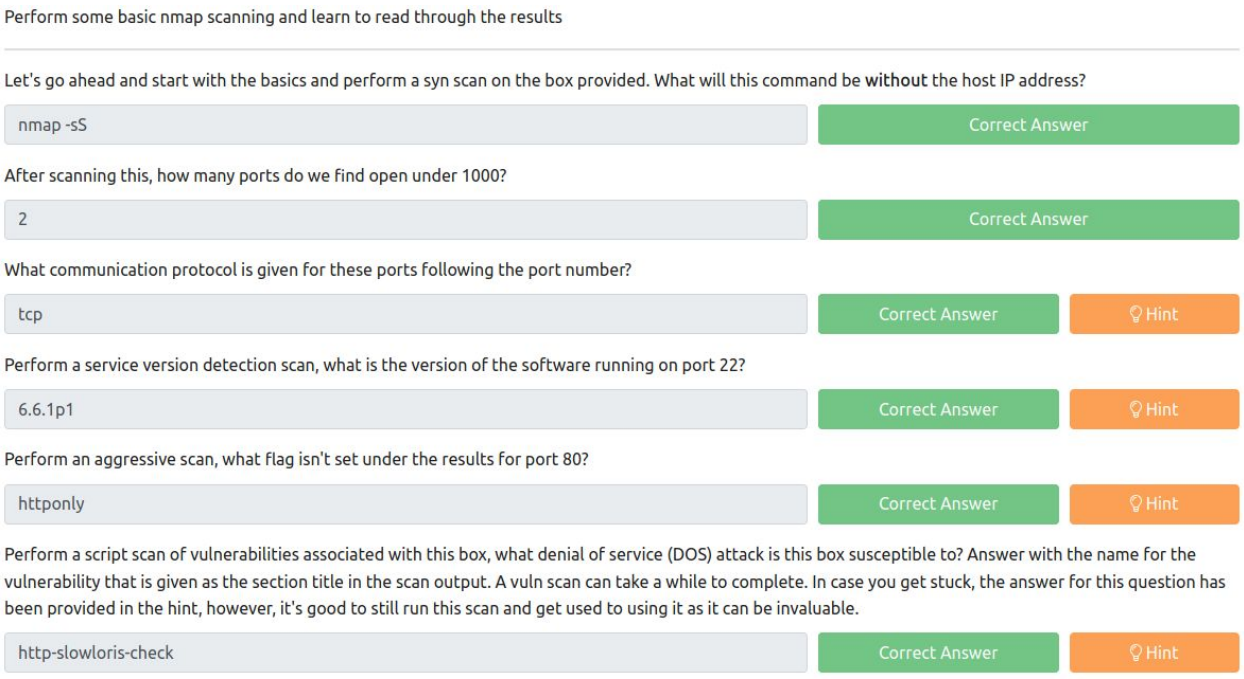
Le but de cet exercice était de trouver un “flag” dans la machine mise à notre disposition, à l’emplacement */passwd*. Nous avons donc essayé d’y accéder grâce à un exécuteur de commande, qui exécutait pour nous des requêtes de type “ping”.

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

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

Nous sommes ensuite passés sur le site tryhackme.org, où nous avons appris à utiliser la commande *nmap*, avec l'aide de Hellblade.



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

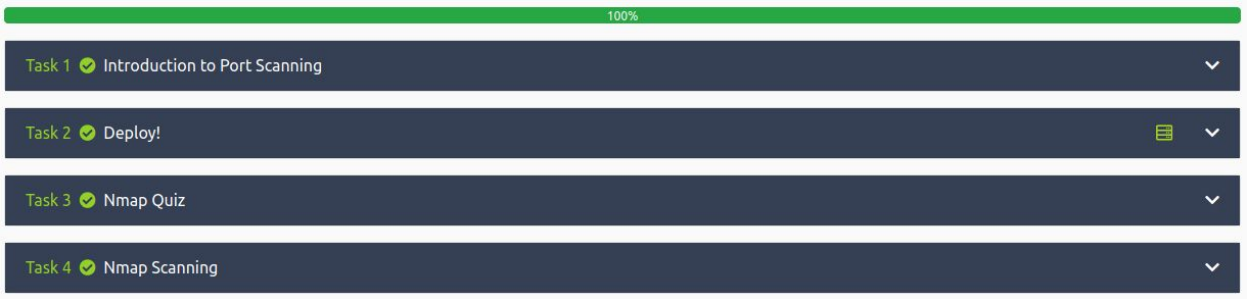
What if I want to run all scripts out of the vulnerability category?

--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.