DÍA D - EJERCICIO FINAL - CTF EXPLOTACIÓN

Canal Slack: cs-ft-sep-23

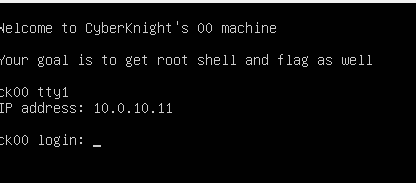
Prerrequisitos

Descargar la máquina "CTF Explotación.ova" del drive de máquinas virtuales e importarla a VirtualBox Encender la máquina virtual y comenzar a trabajar con ella

Explotación

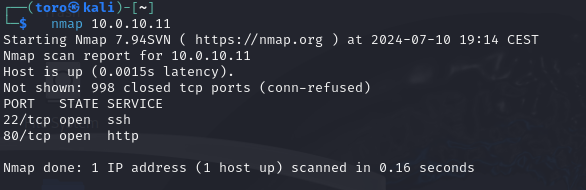
El reto consiste en explotar hasta conseguir una shell y obtener los "flags" correspondientes El resumen de los pasos para completar este CTF se proporciona a continuación:

Obtener la dirección IP de la máquina de destino



La máquina de destino ya nos dice cuál es su IP.

Escanear los puertos usando nmap



Se realizó un escaneo completo de puertos en la máquina de destino para identificar

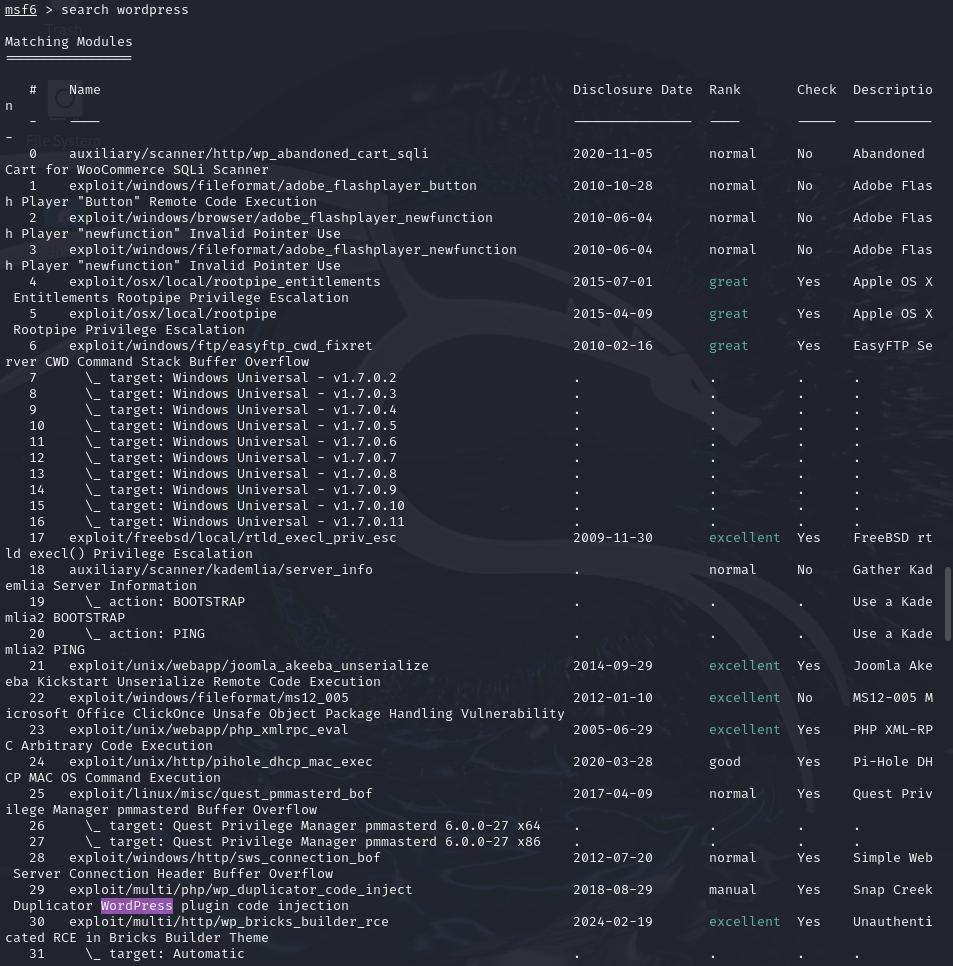
posibles puntos de entrada.

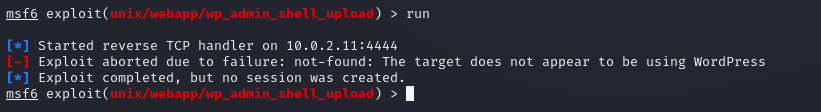
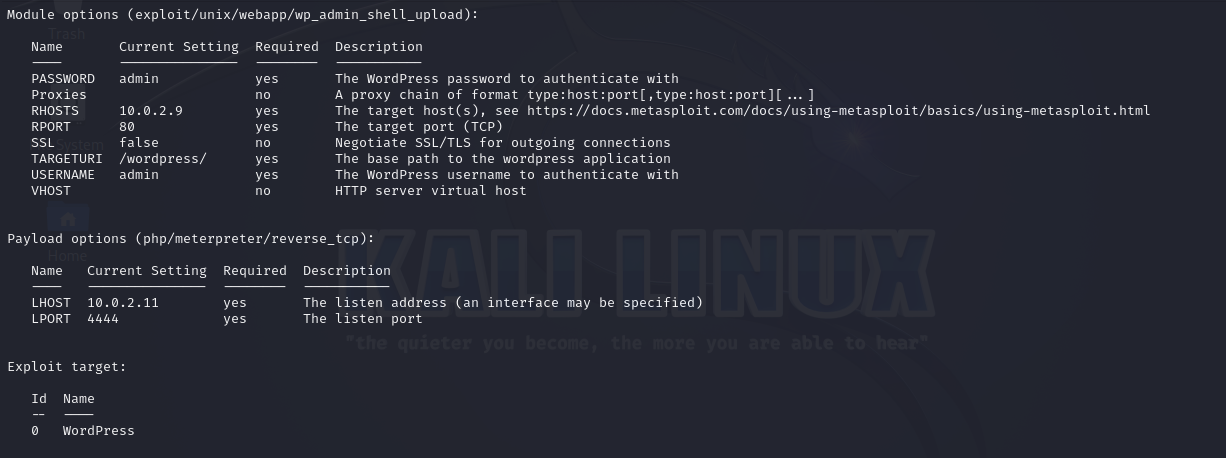
Enumerar el sitio web de WordPress



Se utilizó wpscan para enumerar plugins y posibles vulnerabilidades en el sitio de WordPress.

Explotar usando Metasploit y obtener una conexión Meterpreter





Se buscó y utilizó un exploit para WordPress que permite subir una shell a través de la página de administración pero, después de varios intentos, no se ha conseguido la conexión Meterpreter.

Enumerar el sistema de destino con un shell limitado y obtener los "flags"

Hay que documentar el CTF para realizar la entrega en classroom. Este debe incluir como mínimo: Explicación de como se ha superado cada prueba y/o nivel.

Capturas de pantalla que evidencien como se ha superado cada prueba y/o nivel.