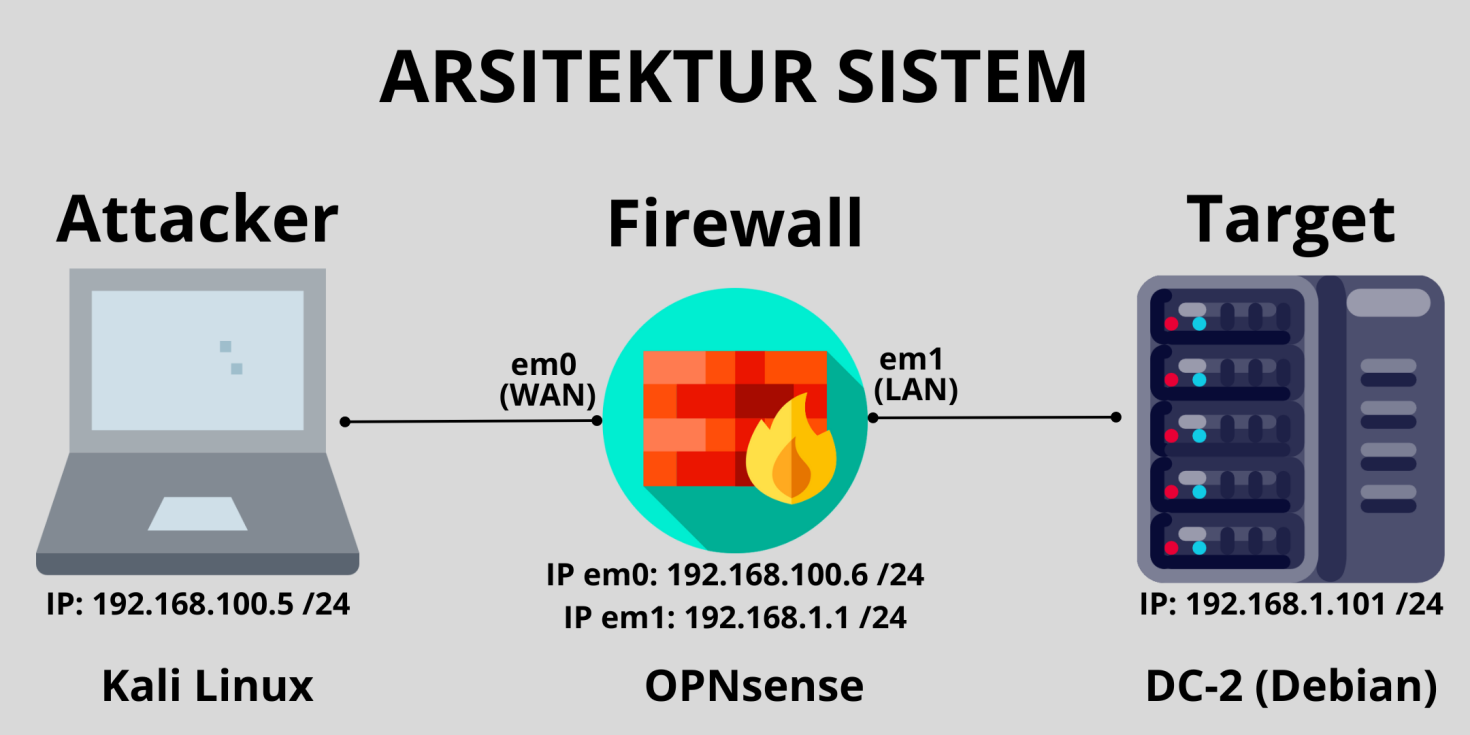
**CTF DC-2**

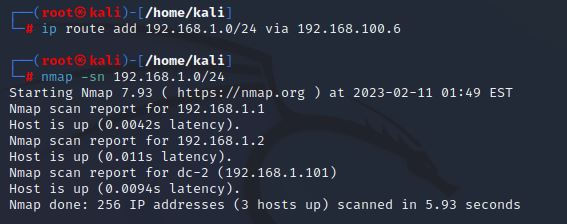
Vulnerable machine: DC-2

<https://www.vulnhub.com/entry/dc-2,311/>



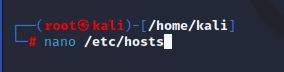
1. Menemukan IP Target

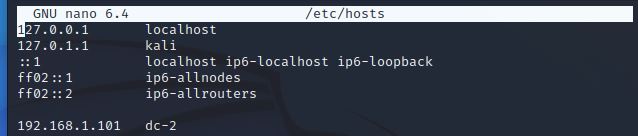
-konfigurasi routing di kali linux dan melakukan scanning pada seluruh network dengan nmap untuk menemukan IP target



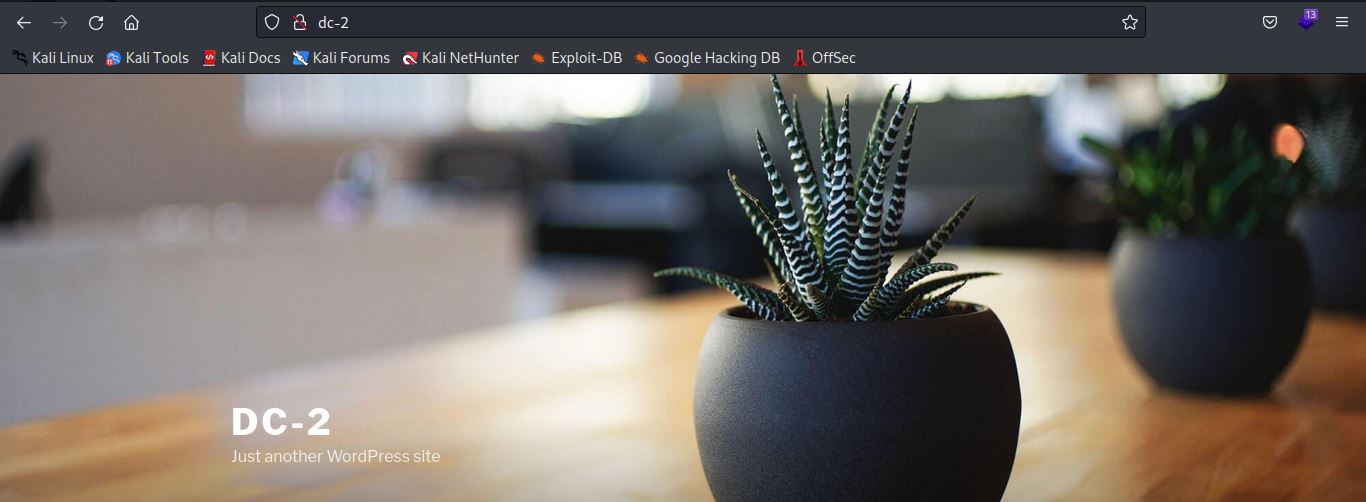
1. Menambahkan IP target pada daftar domain

-menambahkan IP DC-2 pada file /etc/hosts di kali linux

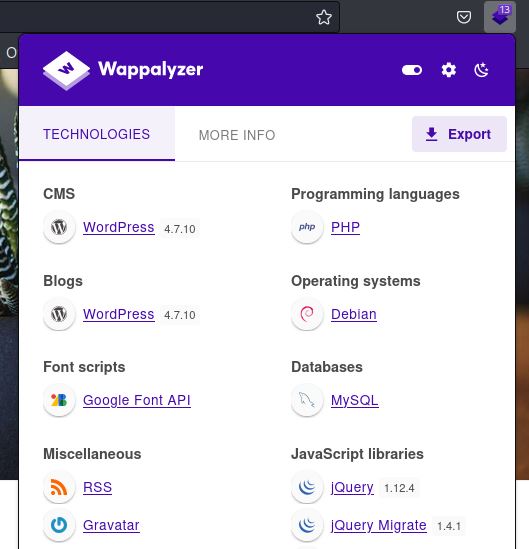




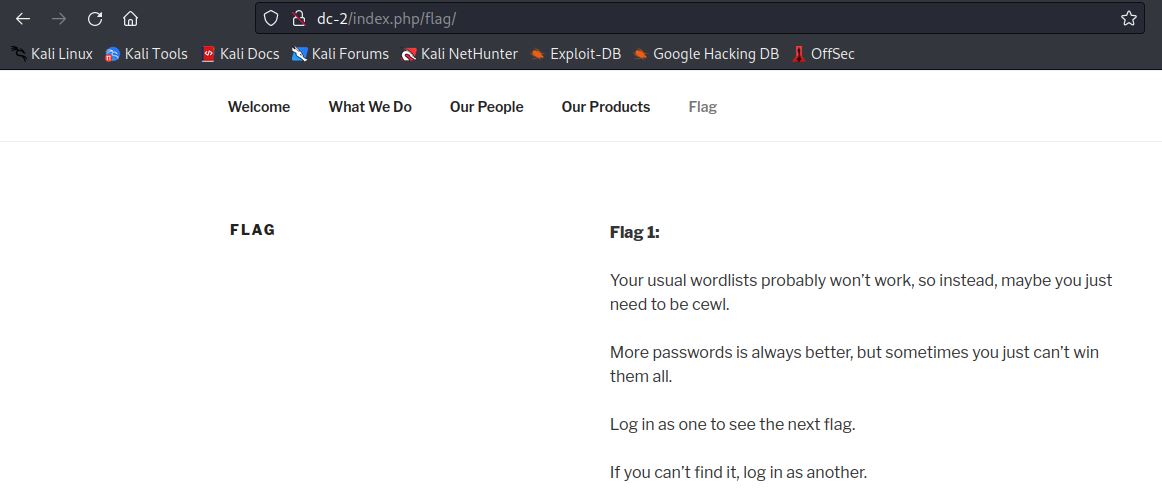
1. Membuka halaman website lewat browser (http://dc-2)



1. Melakukan information gathering dengan plugin firefox “Wappalyzer”



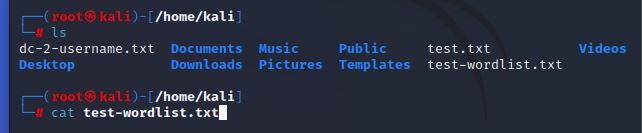
1. Membuat wordlists dengan mengambil semua kata yang ada di website berdasarkan petunjuk di tab flag di website dc-2



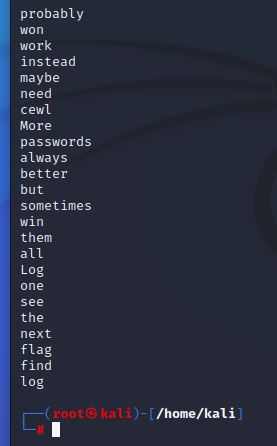
-membuat wordlists dengan cewl

dc-2 6

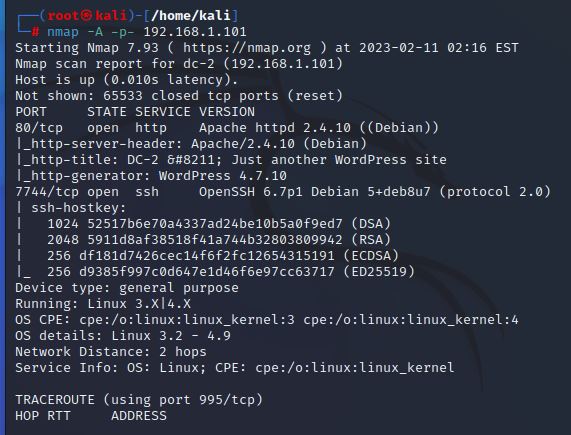
-membaca file hasil wordlists



-melihat isi file wordlist



1. Melakukan scanning seluruh port pada server dc-2 dengan nmap

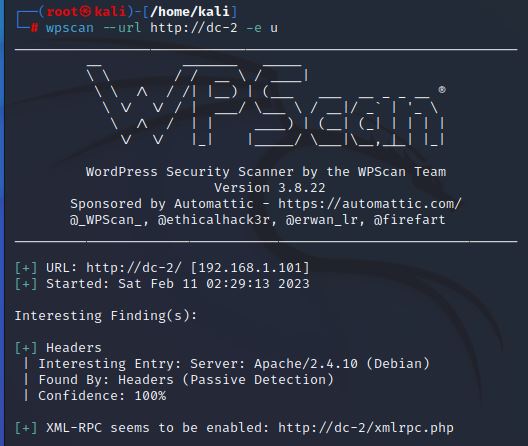


1. Melakukan scanning terhadap halaman wordpress dengan wpscan

-Perintah wpscan --url url\_traget -e emuration

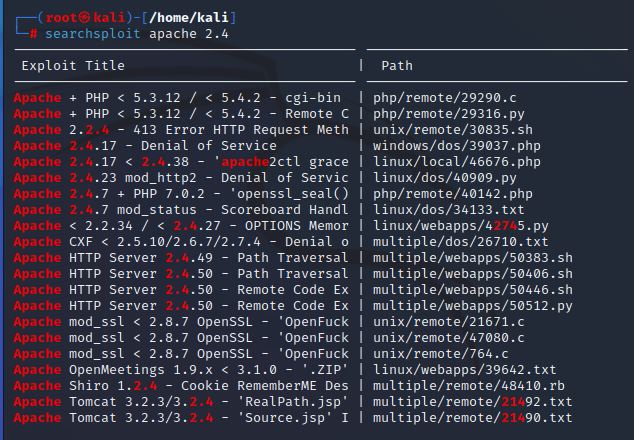


-Melakukan scanning ulang untuk mendapatkan daftar user yang ada di wordpress

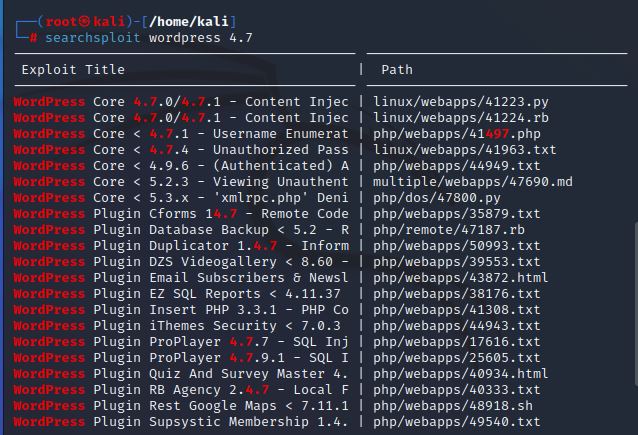


1. Mencari informasi celah pada web server dan CMS yang digunakan berdasarkan informasi yang didapat di wappalyzer dengan searchsploit

-mencari informasi celah keamanan pada apache versi 2.4



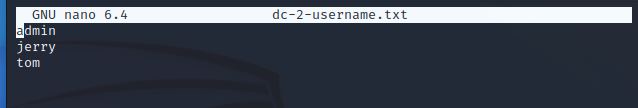
-mencari informasi celah keamanan pada wordpress 4.7



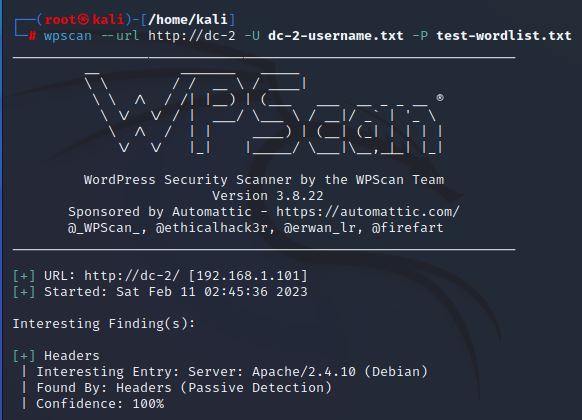
1. Melakukan bruteforce pada website dc-2

-membuat daftar user berdasarkan informasi yang didapat di wpscan

dc-2 15

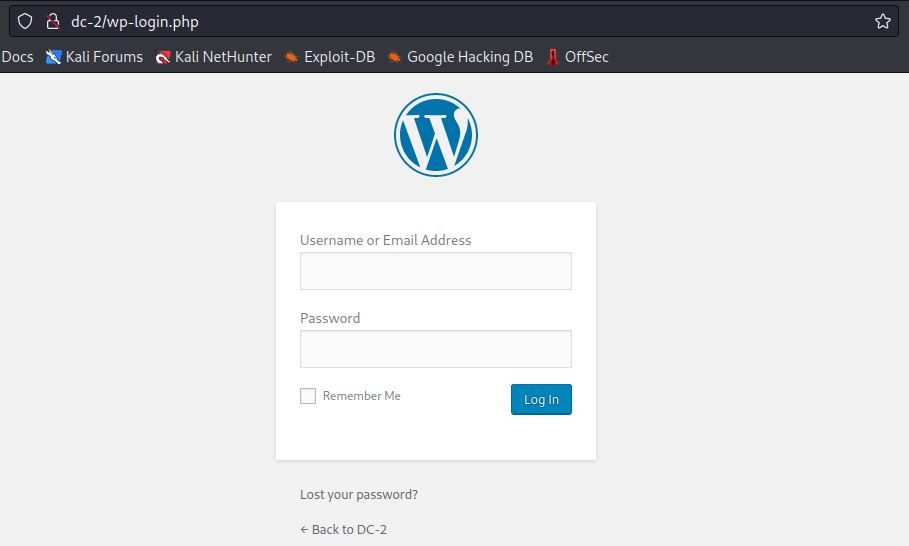


-melakukan bruteforce menggunakan wpscan dengan daftar user dan wordlists yang sudah didapat sebelumnya

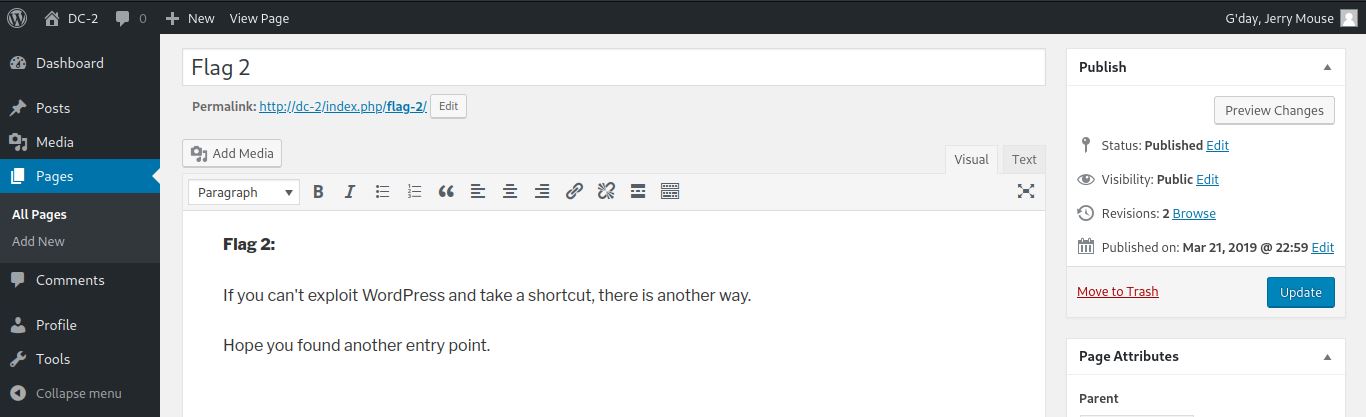


1. Melakukan percobaan login pada website dc-2 berdasarkan username dan password yang sudah didapat saat bruteforce di wpscan

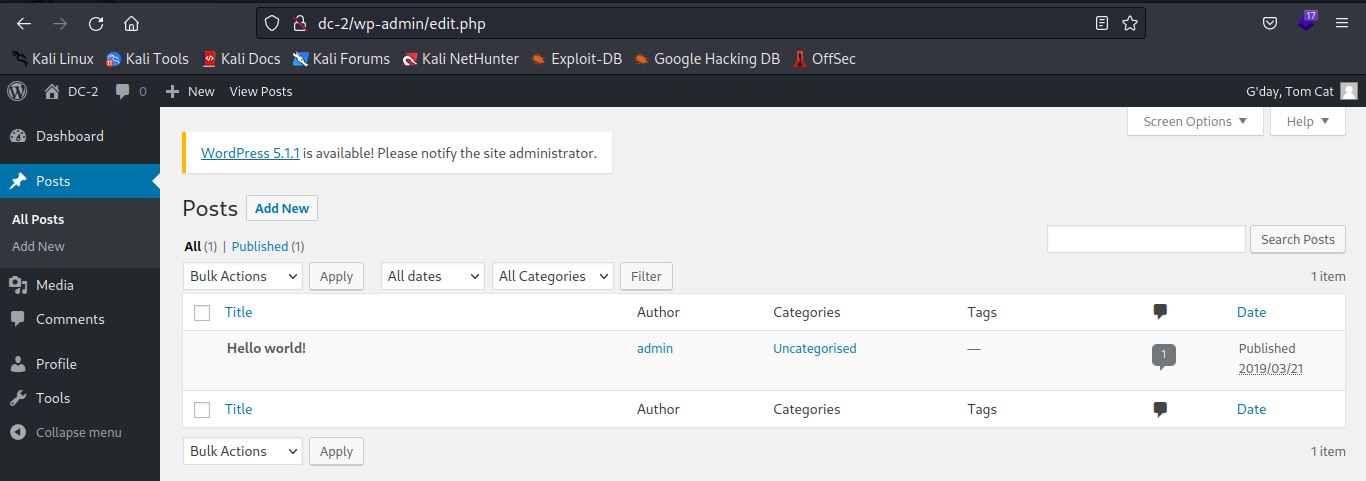
-mengakses halaman login di browser



-login sebagai jerry dan ditemukan flag 2

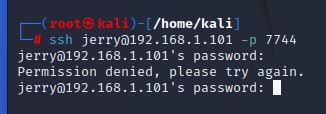


-login sebagai tom

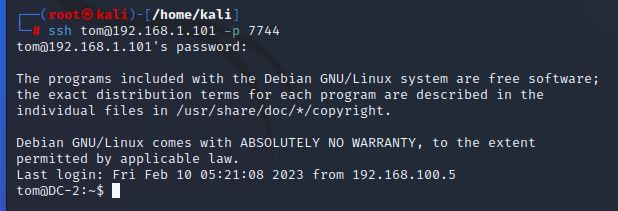


1. Melakukan login SSH dengan asumsi akun yang digunakan sama dengan akun pada wordpress

-mencoba login pada akun SSH jerry

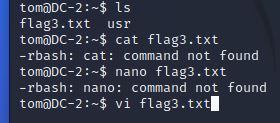


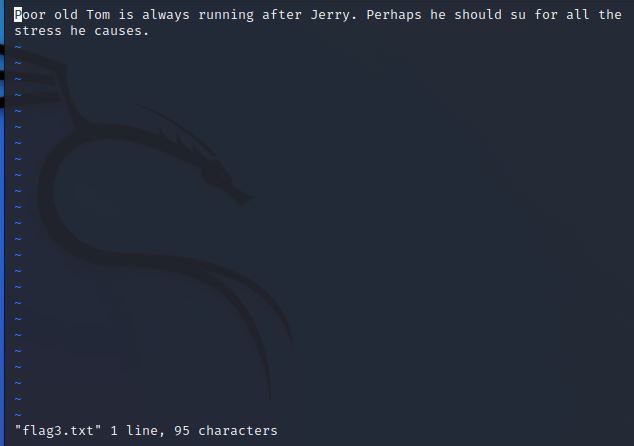
-mencoba login pada akun SSH tom dan ternyata berhasil



1. Milhat daftar file yang dimiliki user tom dan didapat file flag3.txt

-mencoba membaca file dengan perintah cat dan nano namun tidak berhasil



-mencoba membaca file dengan vi editor dan ternyata berhasil

1. Menggunakan vi untuk membuka shell

-ketik :set shell=/bin/bash kemudian tekan enter

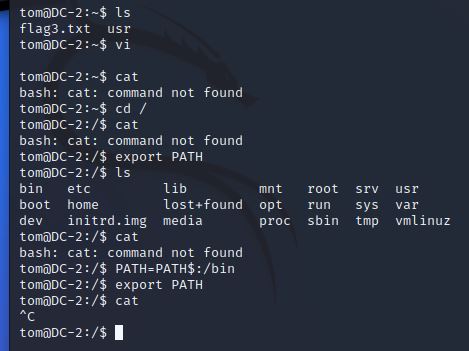


-ketik :shell kemudian enter

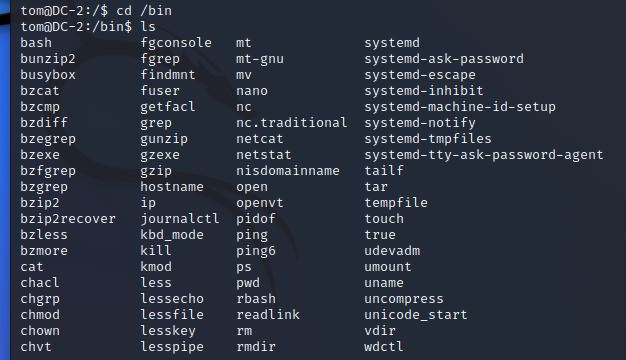


1. Mencoba membuka file flag3.txt dengan cat

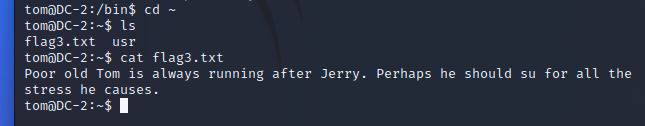
-membuka akses perintah cat



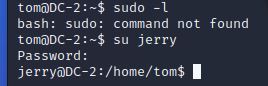
-melihat daftar perintah yang bisa digunakan tom



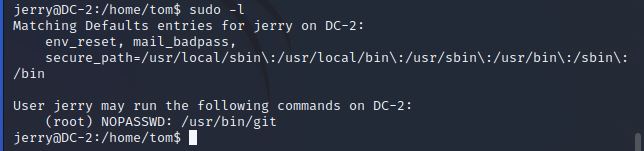
-membaca file flag3.txt dengan cat



1. Melakukan switch user ke akun user jerry dan ternyata berhasil



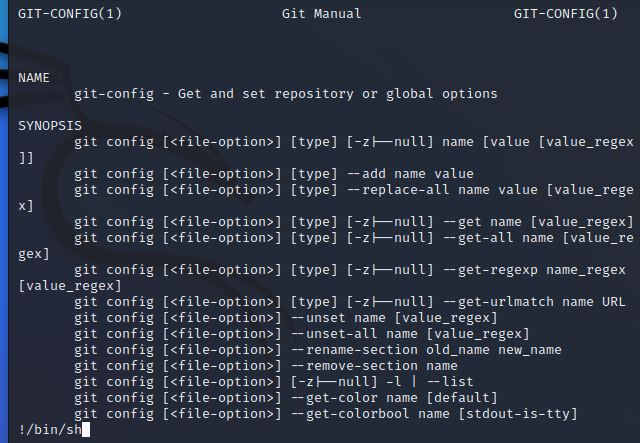
1. Mencari daftar perintah yang bisa dilakukan jerry tanpa akses root



1. Mengubah git menjadi shell

dc-2 32

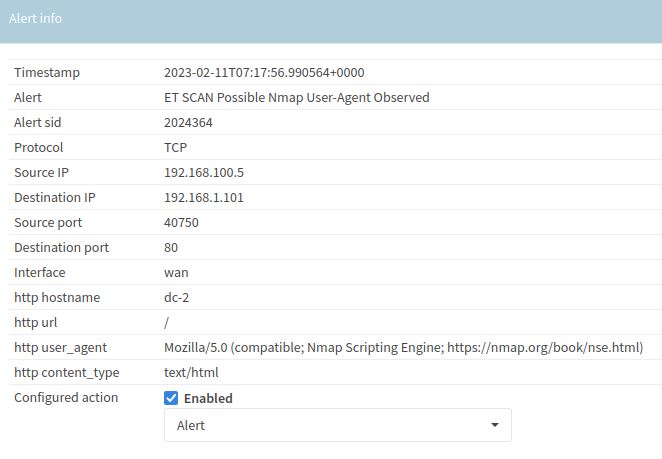
-pada bagian bawah sendiri ubah menjadi !/bin/sh dan tekan enter



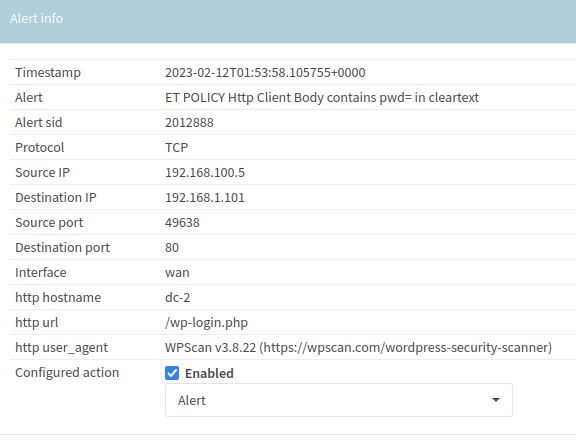
-pada bagian ini telah didapat akses ke terminal root

dc-2 34

Deteksi scanning nmap pada OPNsense



Deteksi penyerangan WPscan pada OPNsense



System Requirement

OPNsense:

-OPNsense 23.1-amd64  
-FreeBSD 13.1-RELEASE-p5  
-OpenSSL 1.1.1s 1 Nov 2022

Kali Linux: 2022.4