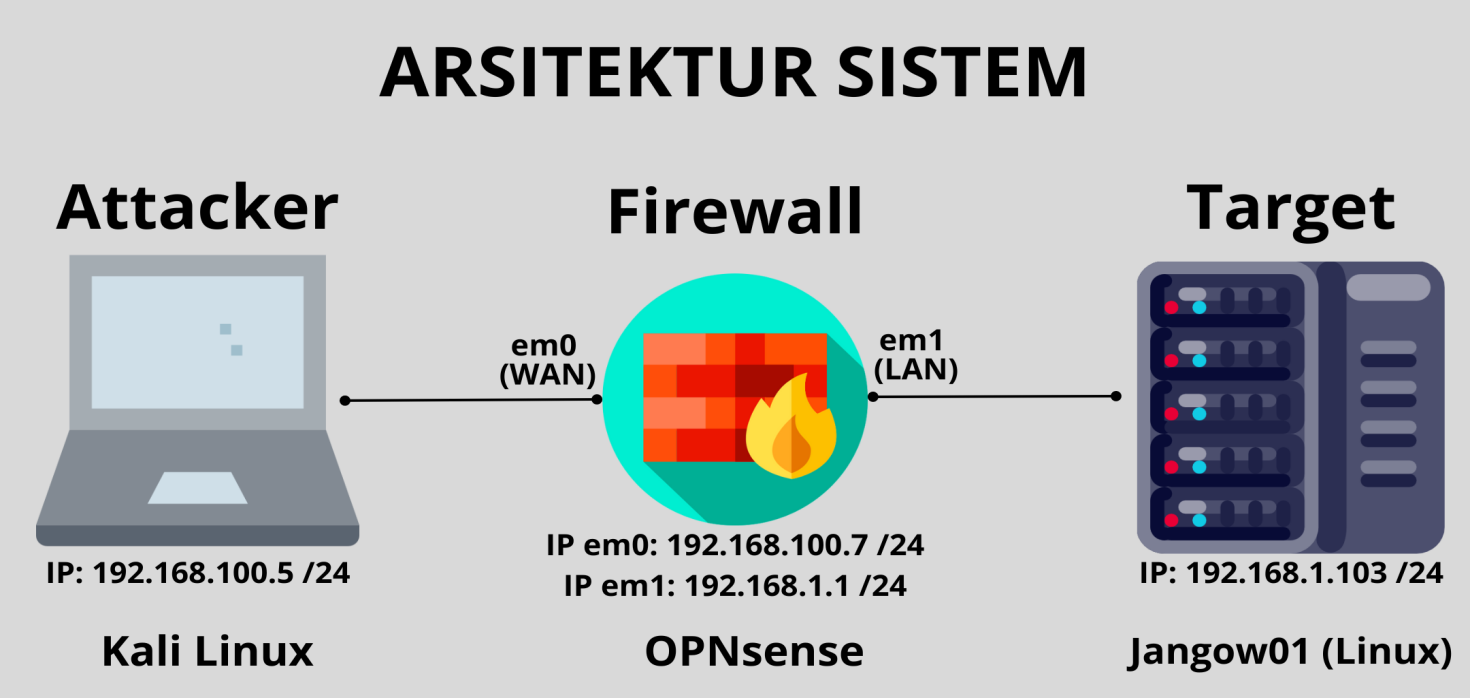
**CTF JANGOW01**

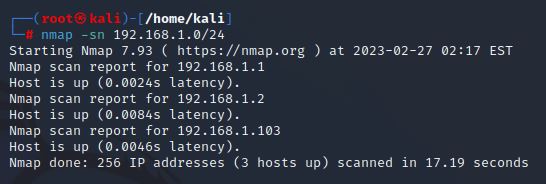
Vulnerable machine: Jangow01

<https://www.vulnhub.com/entry/jangow-101,754/>



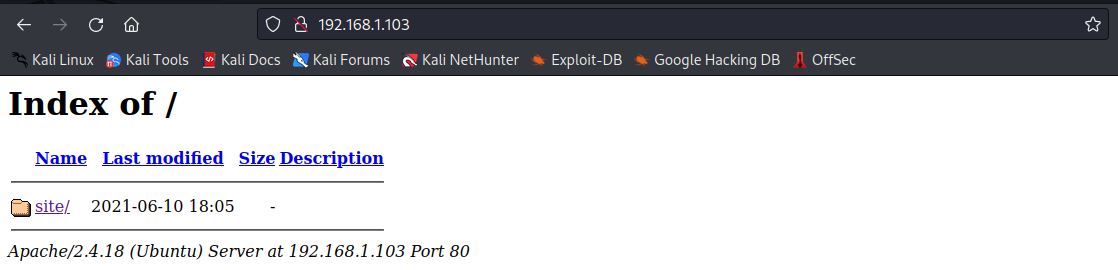
1. Menemukan IP target

- melakukan scanning network dengan nmap untuk menemukan IP target

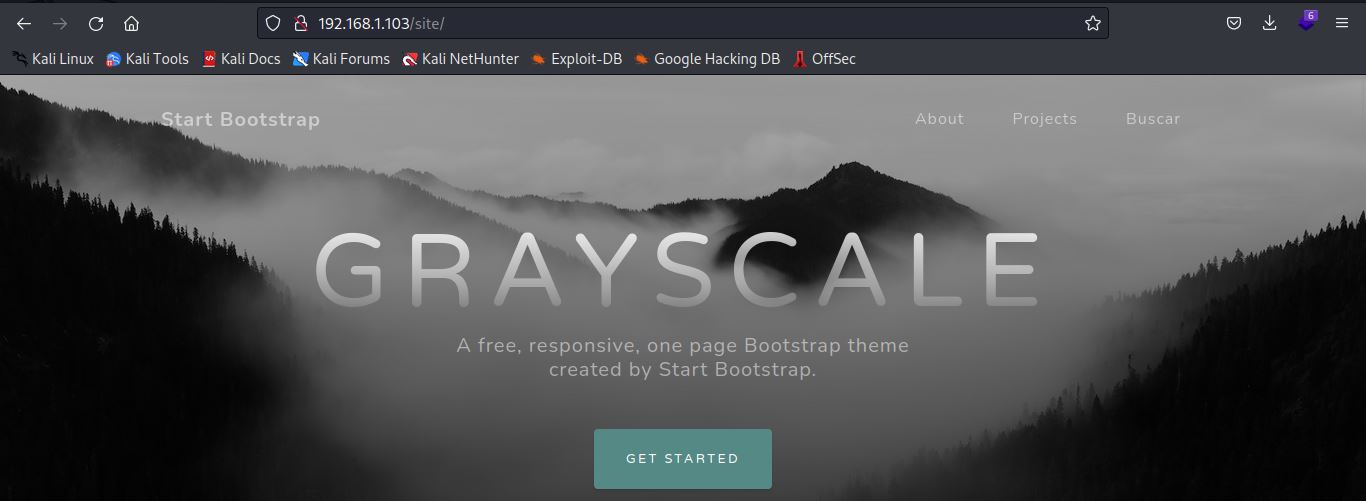


1. Menemukan port yang terbuka pada server

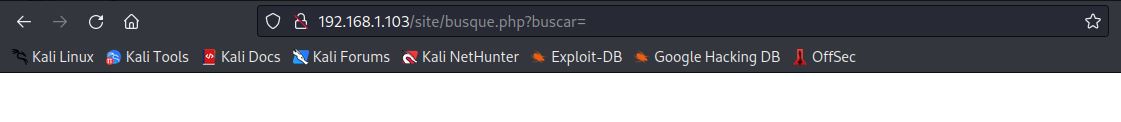


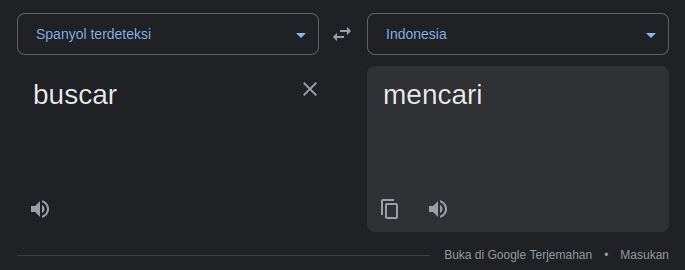
1. Membuka halaman website dengan url http://192.168.1.103

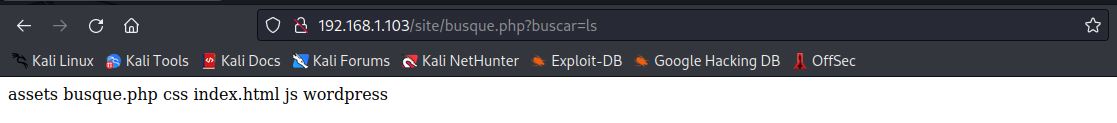
-jika klik folder site maka akan diarahkan ke halaman site



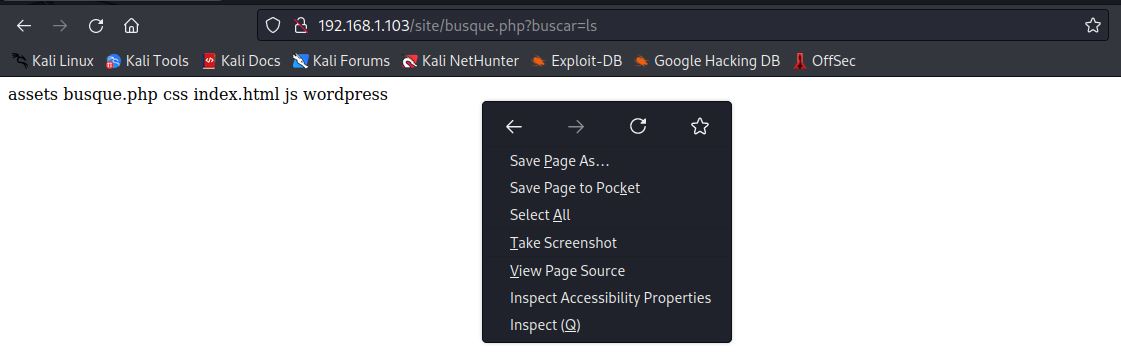
-pada halaman site terdapat menu buscar yang jika diklik akan diarahkan ke halaman kosong

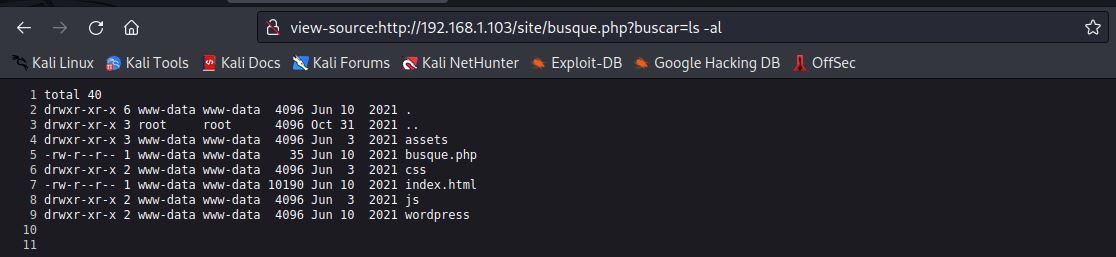
-jika diterjemahkan lewat google translate, buscar adalah bahasa spanyol yang berarti mencari

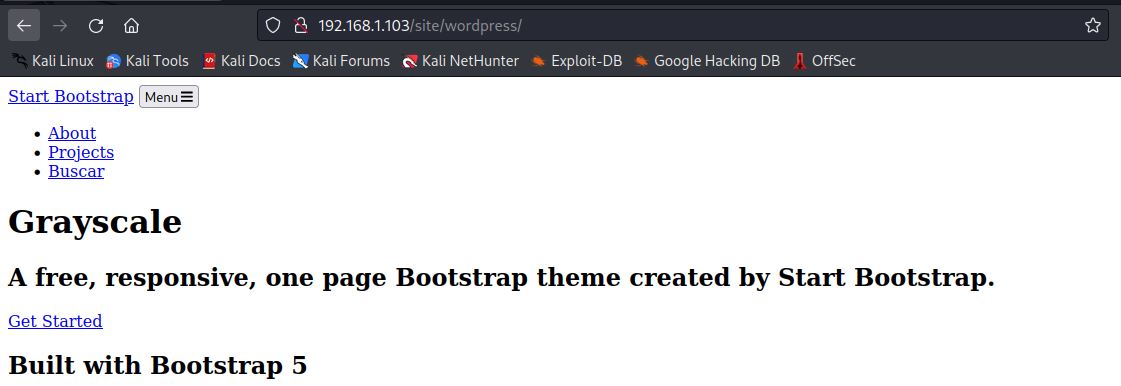


-jadi melalui halaman tersebut kita bisa melakukan remote file inclusion seperti dibawah ini

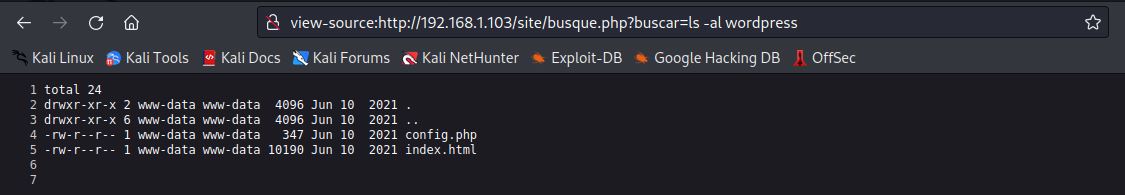
-ubah tampilannya supaya mudah dibaca dengan melakukan klik kanan dan pilih view page source



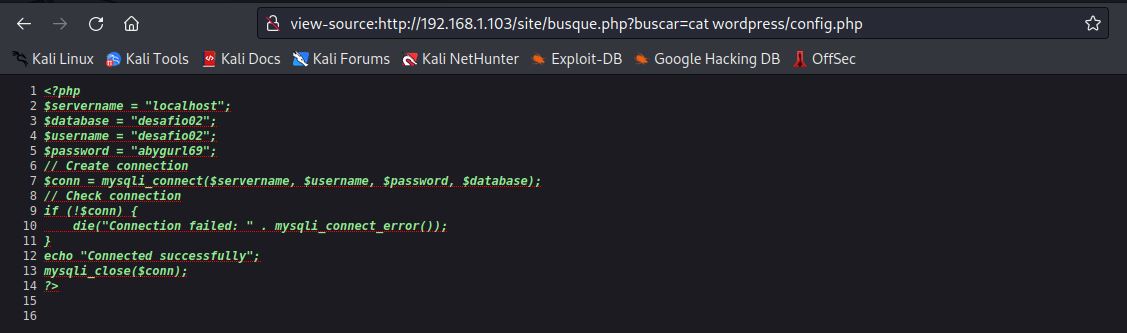
-lihat semua file yang ada pada directory saat ini

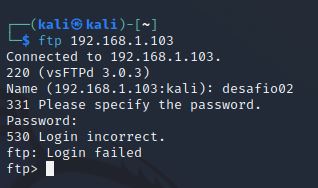
-terdapat halaman wordpress pada website, buka halaman tersebut

-ternyata halaman wordpress tersebut rusak, mungkin karena gagal melakukan koneksi ke database, coba kita explore apa aja isi directory wordpress

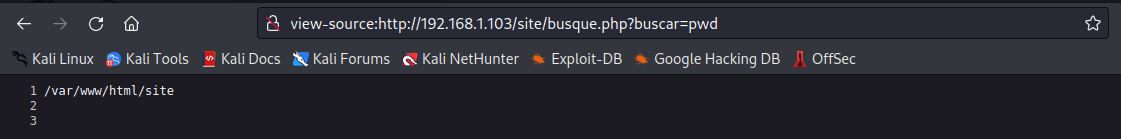


-coba kita lihat isi file config.php dengan perintah cat

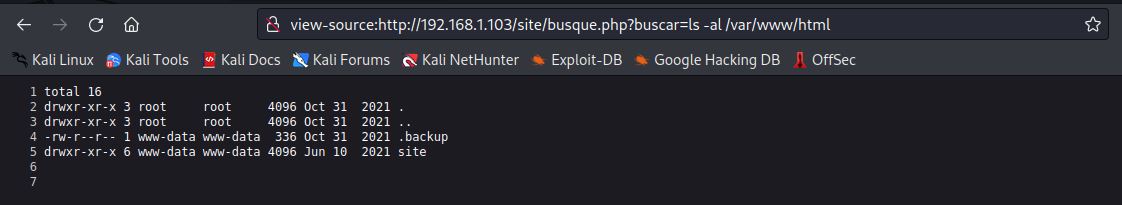
-sekarang kita coba username dan password di file tersebut untuk melakukan koneksi ke FTP Server dan ternyata masih gagal

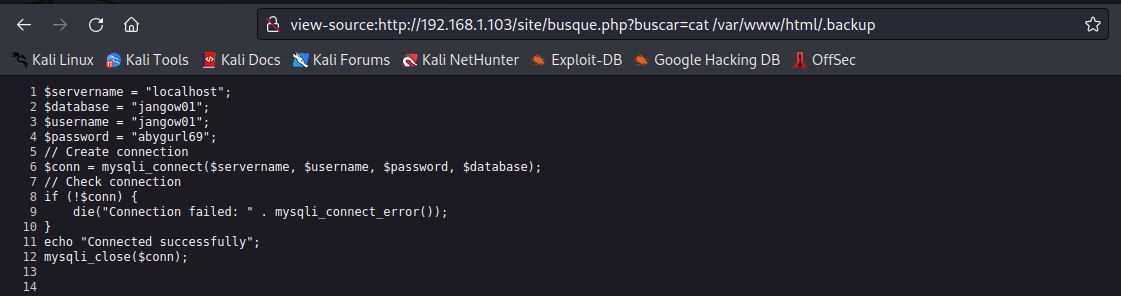


-sekarang kita coba lihat posisi directory saat ini

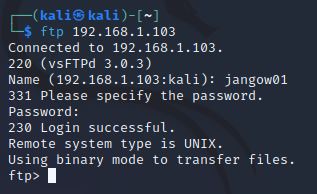


-kemudian kita lihat semua file yang tersembunyi di /var/www/html dan ternyata ditemukan file .backup yang mungkin berisi konfigurasi database



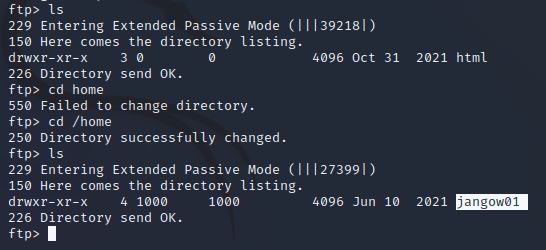
-setelah kita baca dengan perintah cat ternyata isi file tersebut adalah sebagai berikut

-sekarang kita coba lakukan koneksi ke FTP dengan username dan password yang ada file tersebut dan ternyata login berhasil



1. Melakukan explorasi pada FTP

-memindahkan posisi directory ke /root/home dan ditemukan directory jangow01



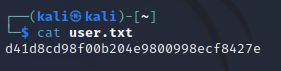
-pada directory jangow01 ditemukan file user.txt



-kita coba download file user.txt melalui FTP

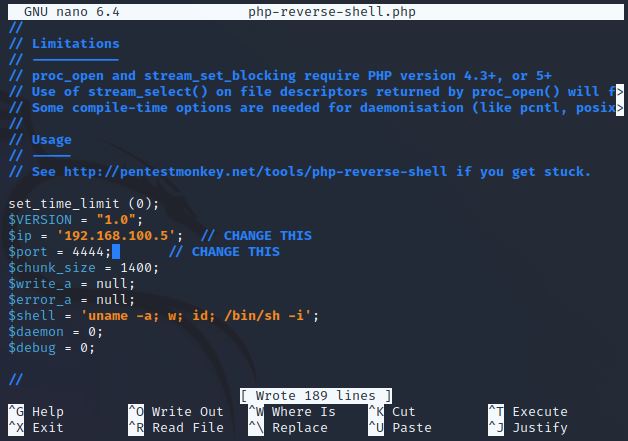


-membaca apa isi file user.txt

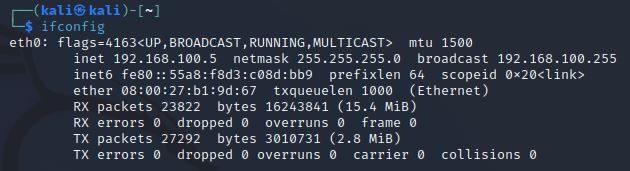


1. Membuat reverse shell untuk mendapatkan akses ke terminal server

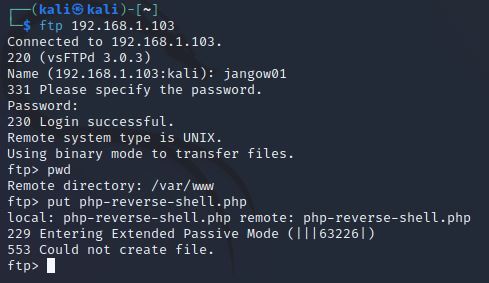
-membuat reverse shell dengan menggunakan bahasa pemrogram PHP (referensi: <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> )



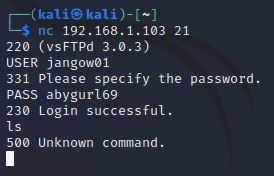
-sesuaikan IP dengan IP di kali linux



-upload reverse shell PHP ke FTP namun user tidak memiliki permission create



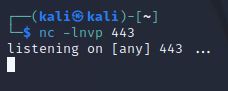
-kita lakukan metode kedua yaitu dengan menggunakan netcat tapi ternyata aksesnya juga terbatas



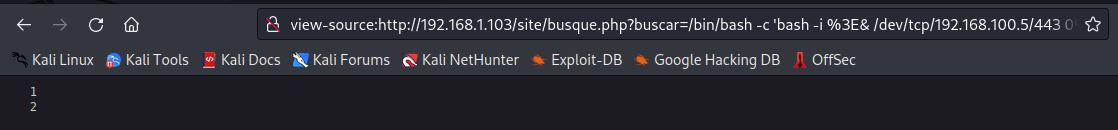
-kita coba metode ketiga yaitu melalui halaman web, pertama-tama kita siapkan kode berikut ini

jg 26

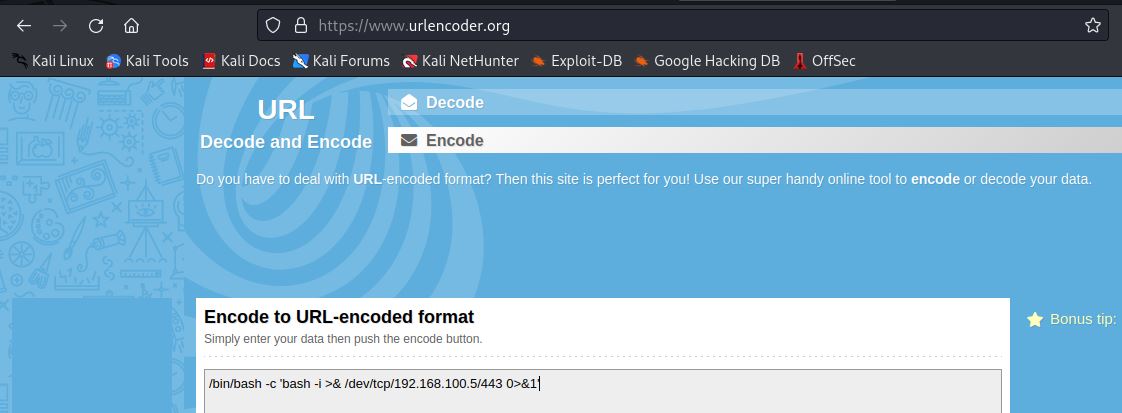
-buat listener pada port 443



-copy script sebelumnya ke url buscar dan tekan enter. Namun disini script terbaca sebagai string



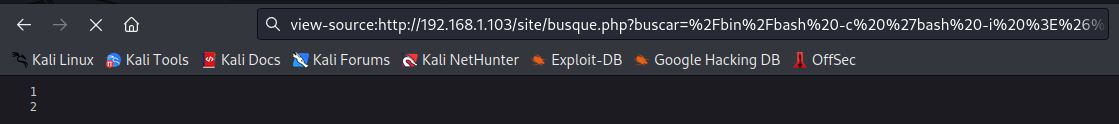
-kita lakukan encode terhadap script tersebut supaya tidak terbaca sebagai string melalui <https://www.urlencoder.org/>



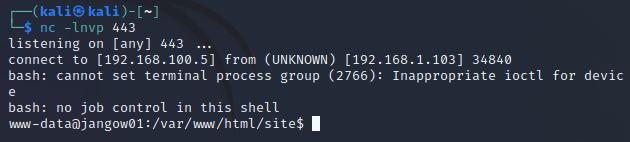
-berikut ini adalah hasil encode



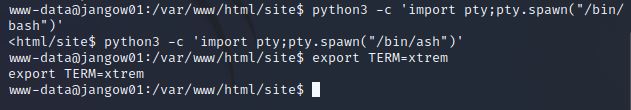
-copy hasil encode ke url sebelumnya dan tekan enter



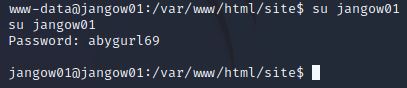
-reverse shell berhasil berjalan



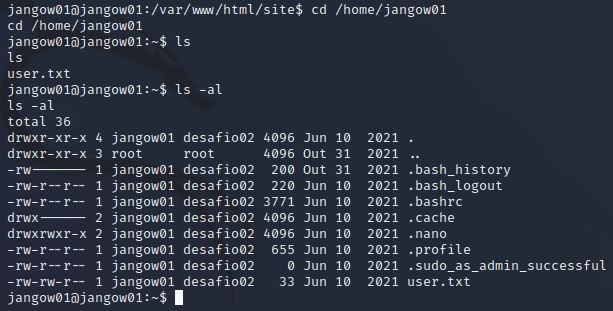
1. Buat reverse shell menjadi interactive terminal dengan phyton



1. Melakukan switch user ke user jangow01 dengan password sebelumnya

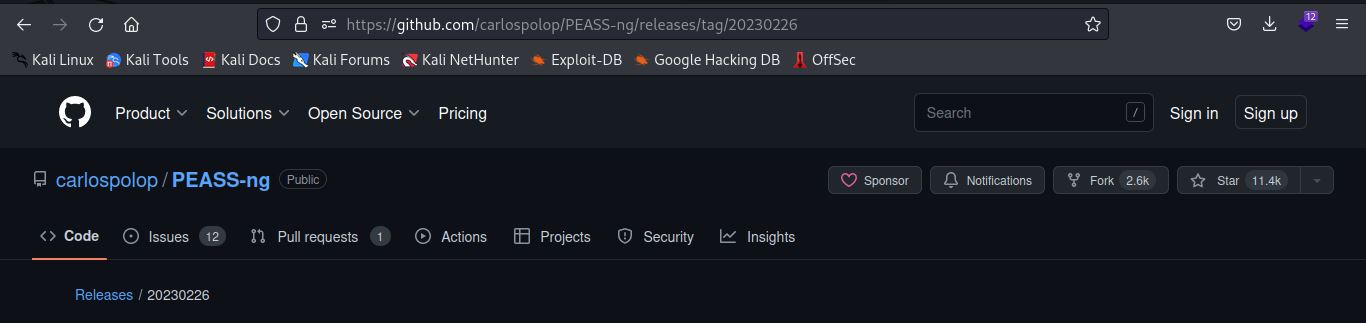
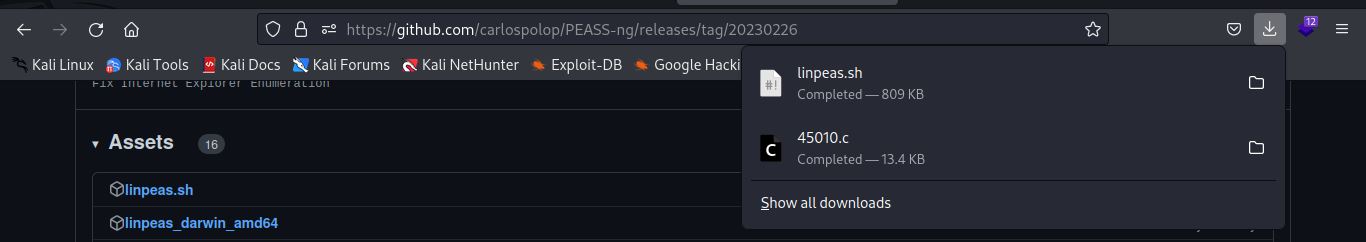


1. Pindah ke directory user dan melihat ada file apa aja didalamnya

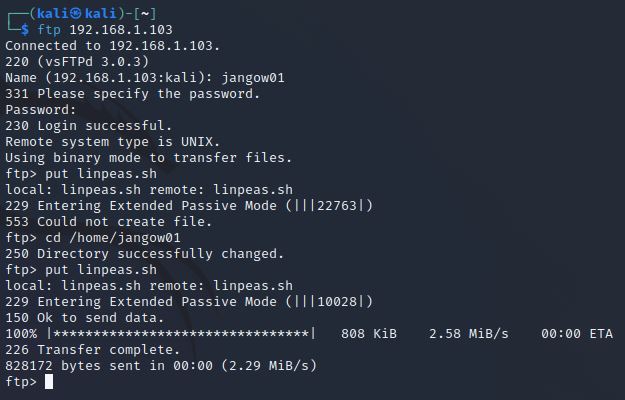


1. Melakukan privilege escalation terhadap server

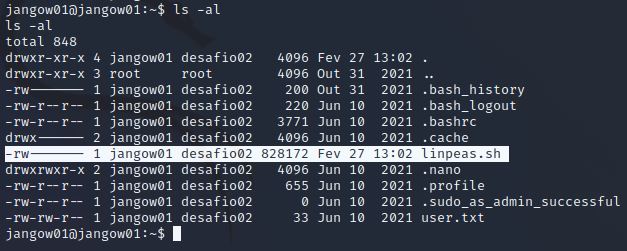
-download bash script linpeas.sh di github <https://github.com/carlospolop/PEASS-ng/releases/tag/20230226>



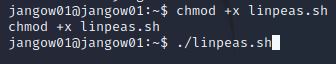
-upload file linpeas.sh ke server dengan FTP



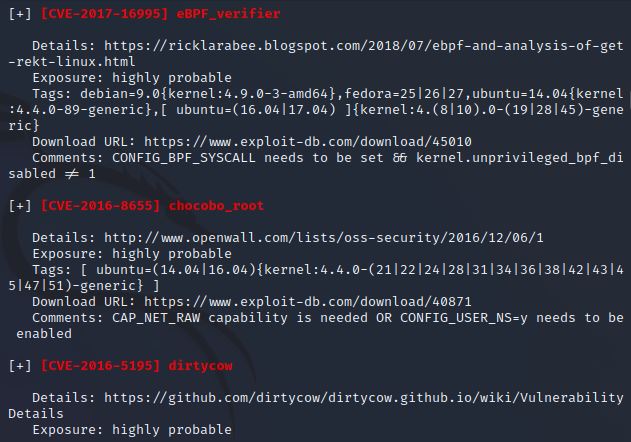
-file berhasil terhasil terupload ke server



-tambahkan permission execute dan jalankan file tersebut di server

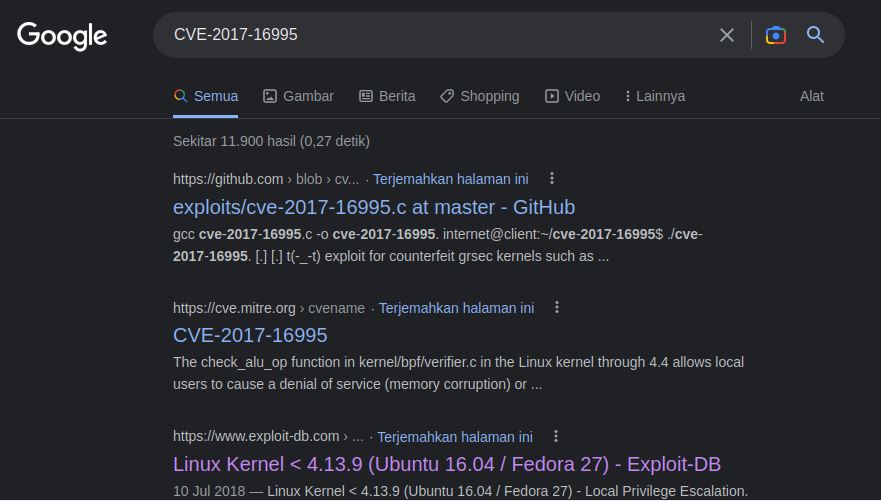


-setelah dijalankan ternyata server rentan dengan serangan CVE-2017-16995

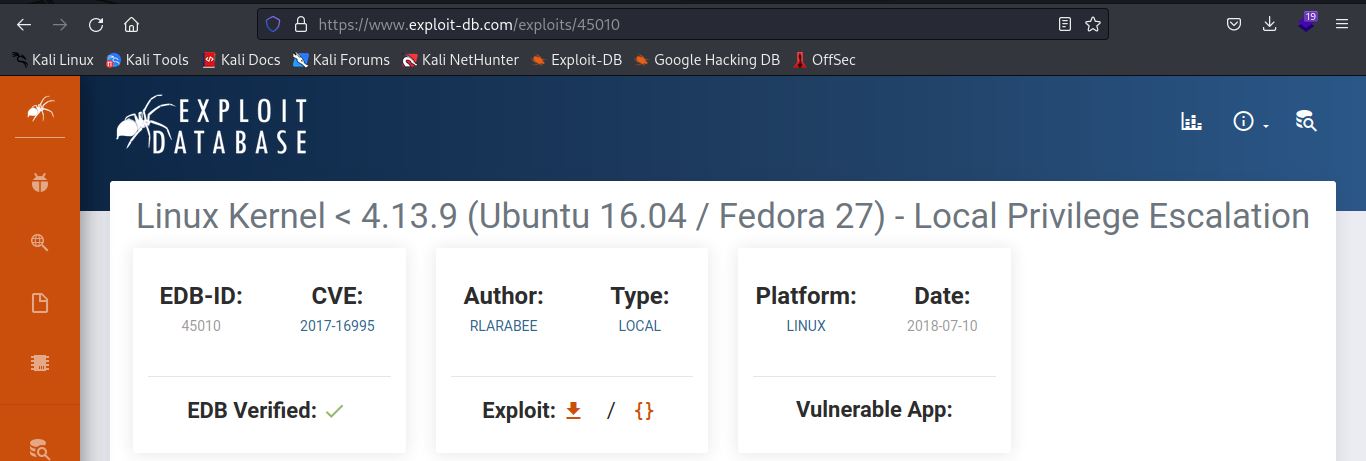


1. Meretas server dengan CVE-2017-16995

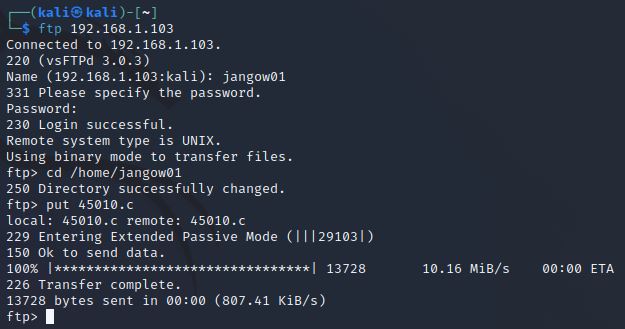
-cari tahu informasi CVE-2017-16995 di google



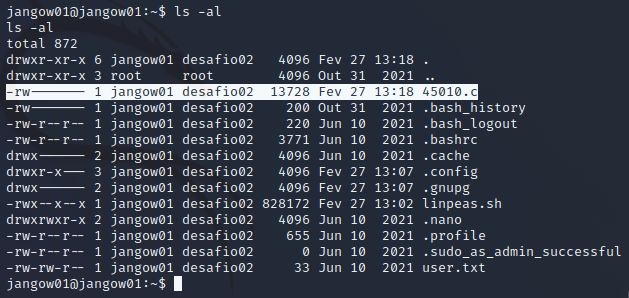
-download file exploit CVE-2017-16995 di <https://www.exploit-db.com/exploits/45010>



-upload ke server dengan FTP



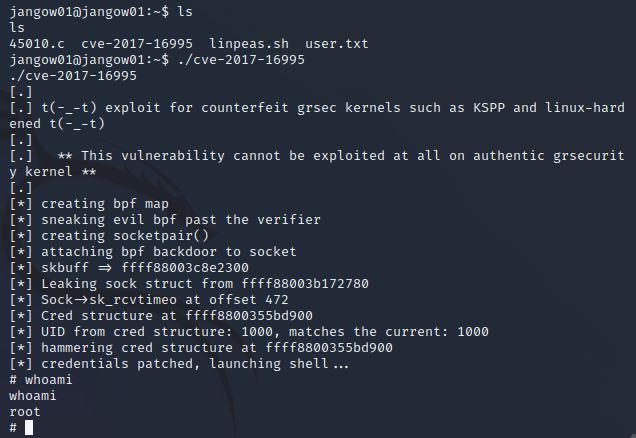
-file berhasil terupload ke server



-lakukan proses compile pada file tersebut

jg 46

-setelah proses compile berhasil, jalankan file cve-2017-16995. Dari sini kita dapatkan akses ke terimal root



System Requirement

OPNsense:

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

Kali Linux: 2022.4