Kucam prvo komandu ifconfing na svom kali linux-u

Text

Description automatically generated

I kali linux ce pokazati ip adresu racunara na kojem radim i netmask koji govori da smo u klasi C subnetu tj. /24

Tako da cemo koristiti nmap komandu da skeniramo sve ip adrese na ovom subnetu i probati uraditi host detekciju

Text

Description automatically generated

Rezultat nam vraca 3 adrese

Prvu adresu kad poredimo sa nasom zakljucujemo da je to defaultna getaway adresa

Druga adresa je nasa

Treca je adresa poslije nase i nju cemo skenirati

Radimo nmap SYN stealth scan sa sudo jer nam trebaju root privilegije

Text

Description automatically generated

Vidimo da imamo tri otvorena porta 21, 22 i 80 (ftp, ssh, http)

Radimo servisnu enumeraciju na otvorene portove

Text

Description automatically generated

Za port 21 radi se o ProFTP deamonu

Za port 22 imamo OpenSSH 8.2p1 Ubuntu

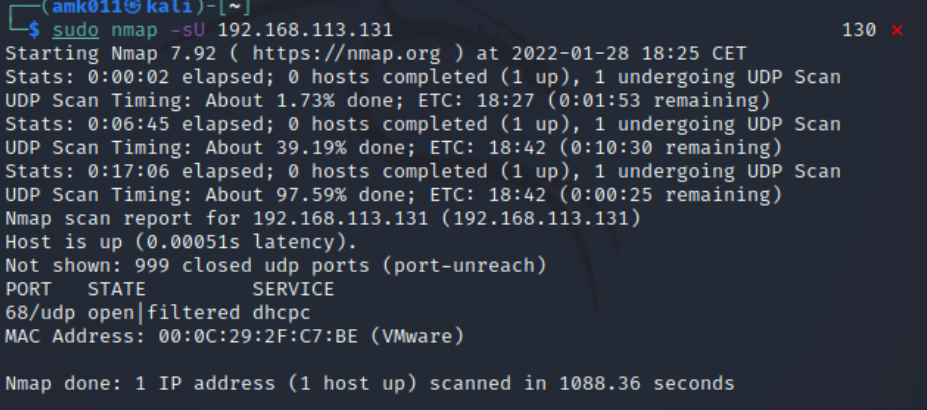
Za port 80 vidimo da se radi o Apache http deamonu 2.4.41 Ubuntu (2.4.52 lastest verziaj)

Vidimo da file transport protokol omogucava anonymous login i ne koristi enkripciju. Preporucujemo koristenje FTPS sa enkripcijom ili SFTP.

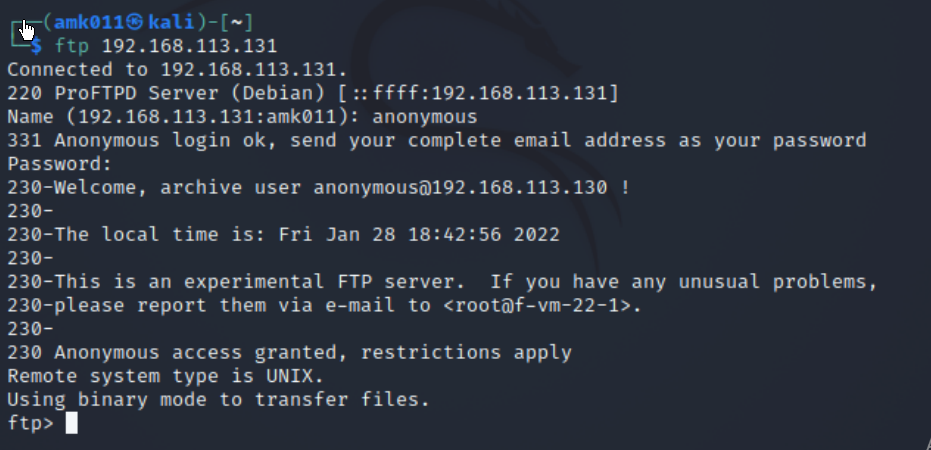
Uradio sam i UDP skeniranje

Pa smo nasli jedan port 68 open | filtered dhcpc servis koji služi za dinamično alociranje ip adresa prilikom bootanja

Preporucujemo koristenje jaceg firewalla koji ce kontolirati portove I njihovu vidljivost i koristenje PORTSPOOF alata za dodatnu zastitu servisa.

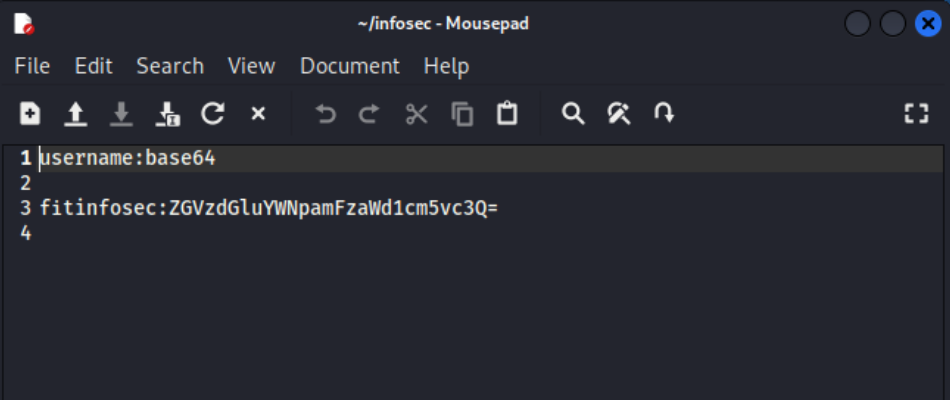


Vidimo da je Anonymous ftp login allowed pa cemo pristupiti ftp-u i sacuvati fajlove koji su prikazani



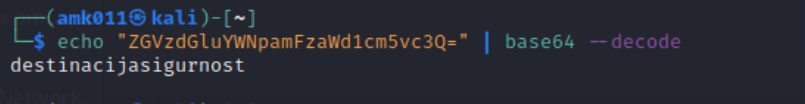
Pomocu komande mget skinuli smo fajlove u defaultni folder tj u ovom slucaju /home

Prvi fajl je samo ova welcome poruka ali u drugom fajlu imamo korisnih informacija

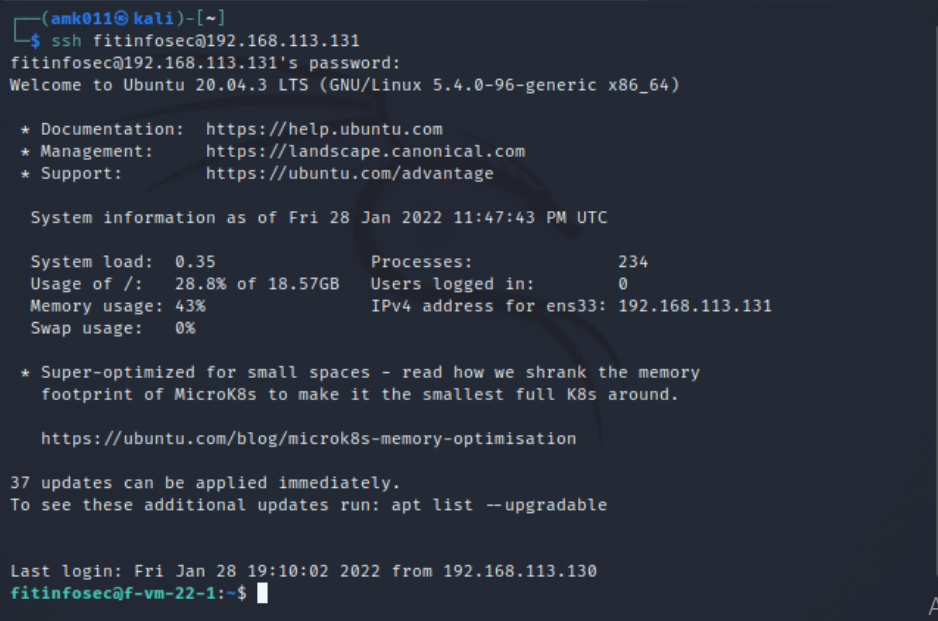


Imamo hint da je usernam fitinfosec a pass u enkodiranom formatu

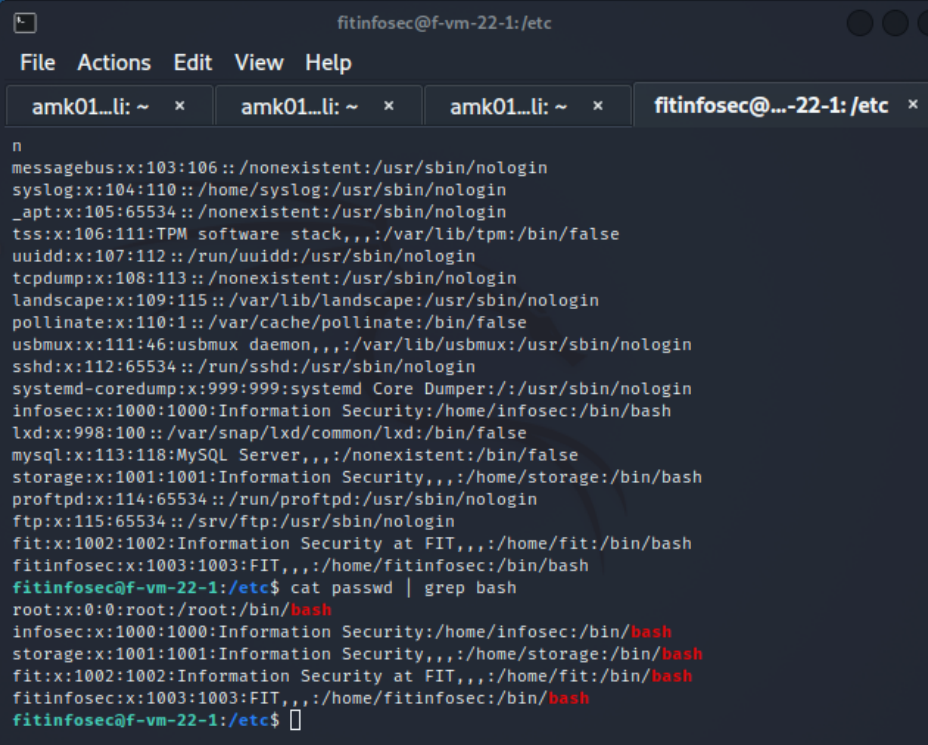
Na jednostavan nacin mozemo da dekodiramo poruku i dobijamo pasvord za usera



Logiramo se sa tim podacima

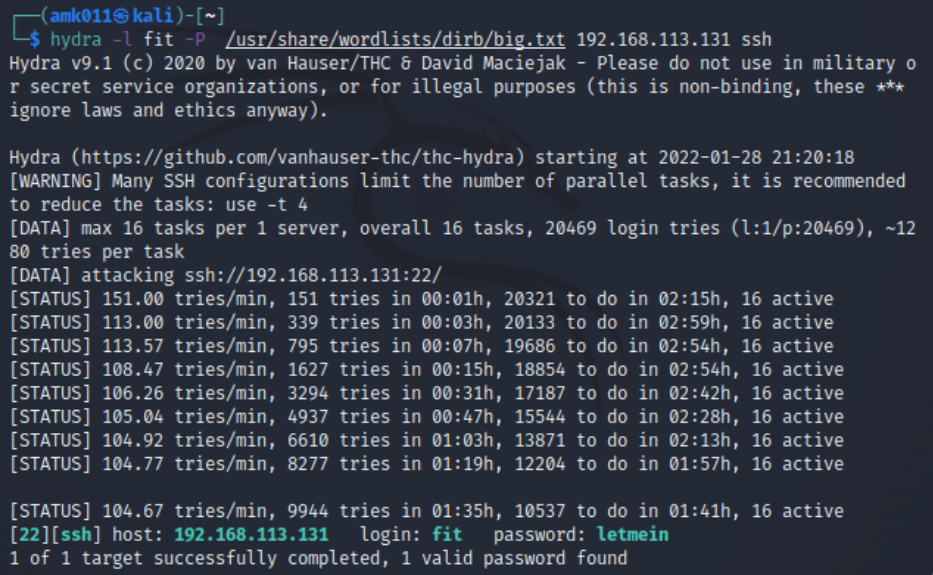


Prolaskom kroz direktorije dolazimo u etc i komandom cat ispisujemo ostale usere iz filea passwd



Koristio sam brute force sa hydrom i hashcatom pronasao jos 2 password-a za 2 usera

Za username fit password je letmein



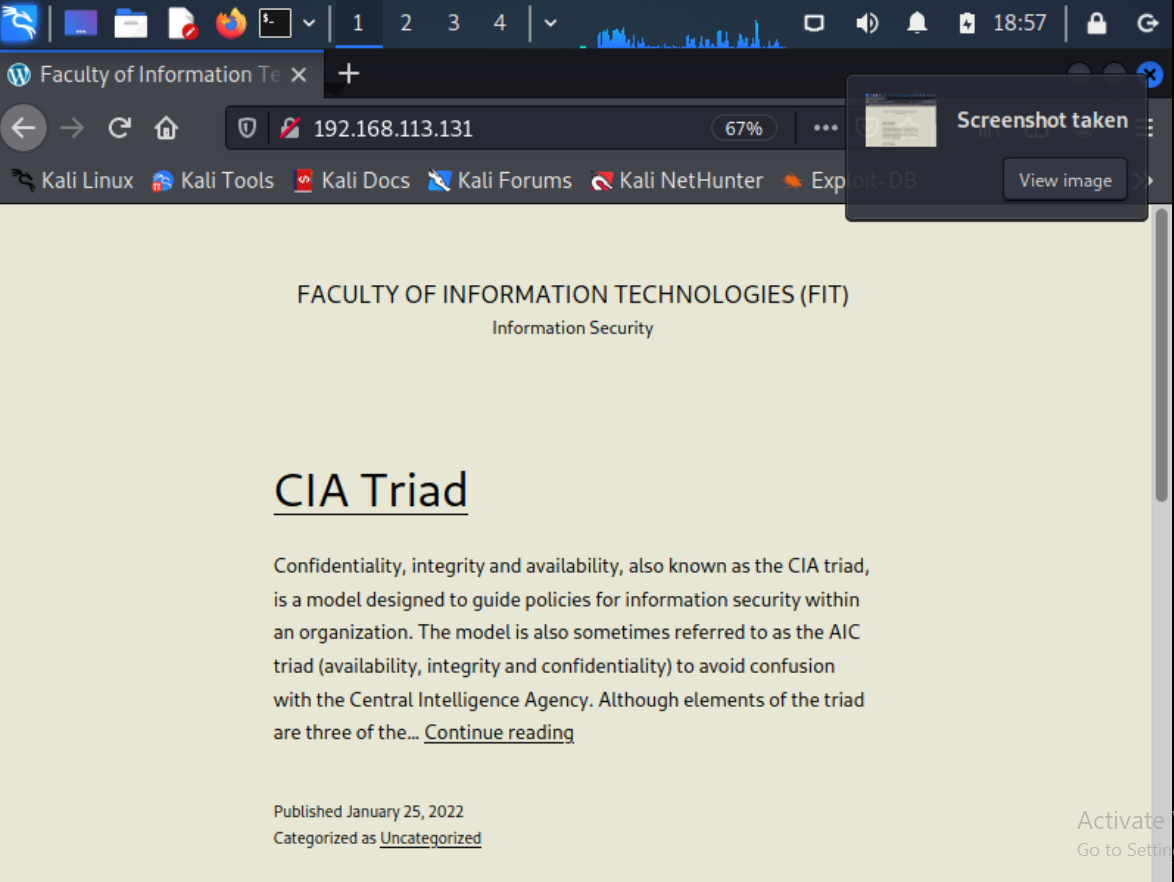
A za storage password je trex, tu sam koristio hashcat, etc/shadow nasao hash vrijednost usera

Text

Description automatically generated

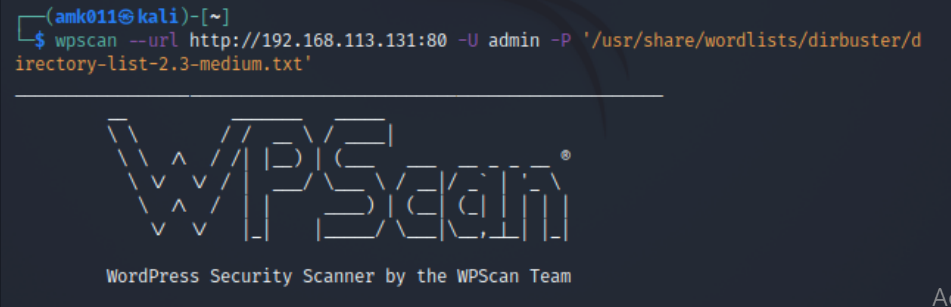
Text

Description automatically generated

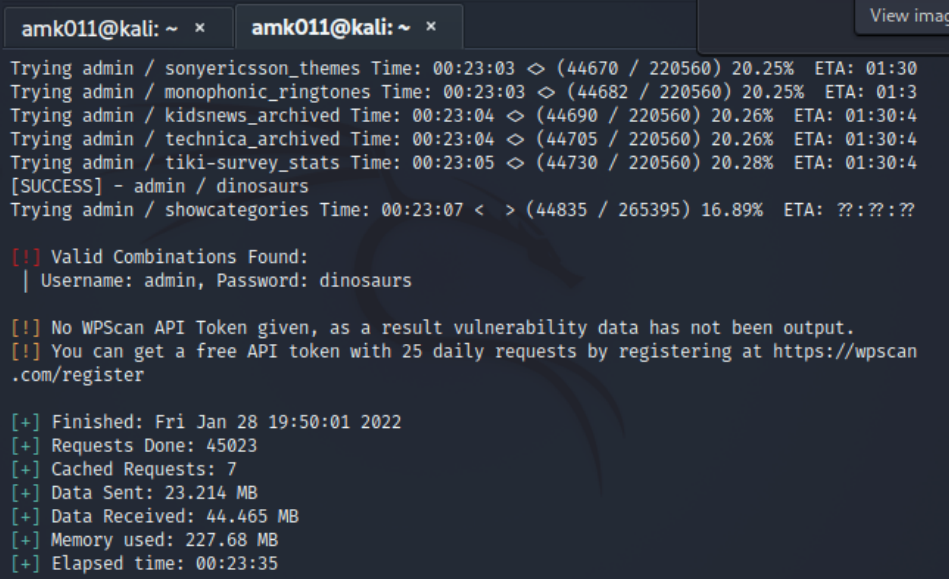
Otvaramo web stranicu koja je na portu 80 preporucujemo koristenje HTTPS(TLS enkripcija) jer kod HTTP protokola svi nekriptovani podaci se mogu interaptat 

Na stranici vidimo post od admina

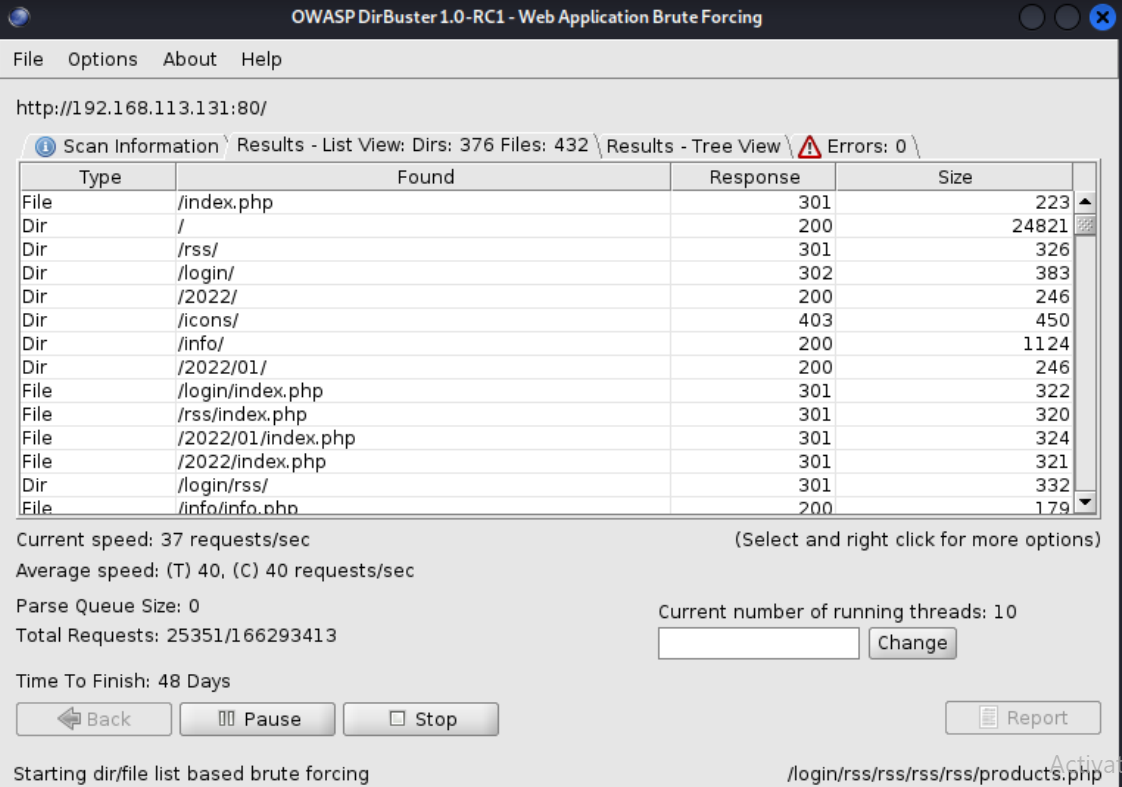
Pokrecemo wordpress skan za admina



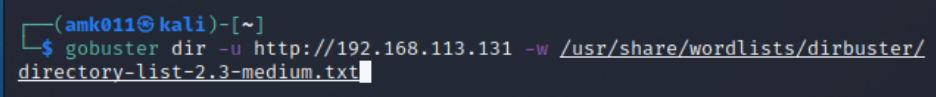
Pronalazimo passwrod dinosaurs



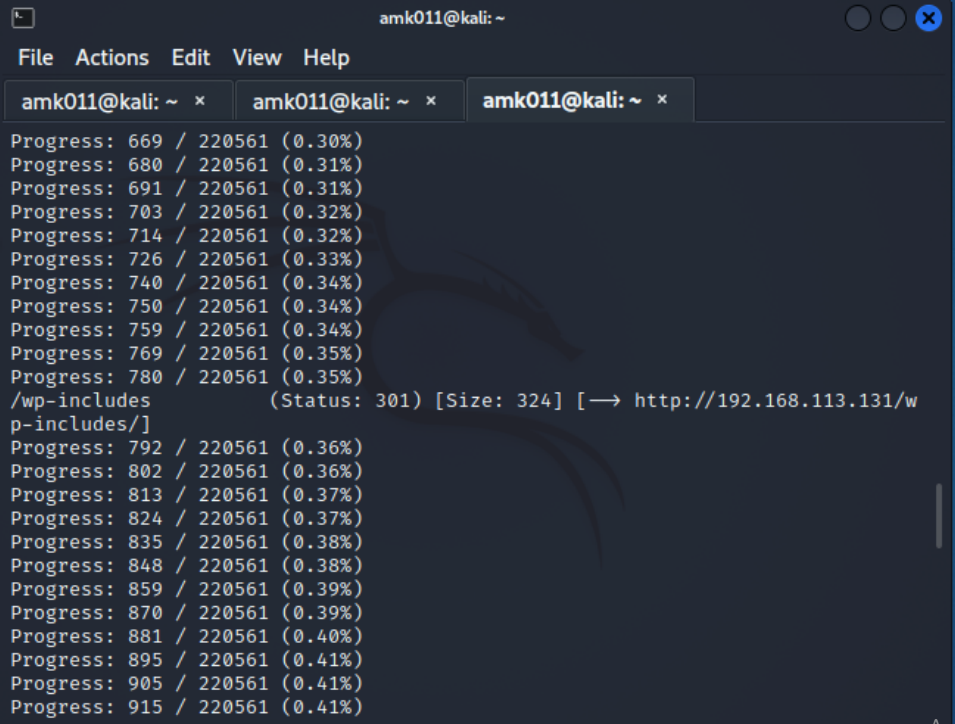
Pokrenuo sam dirBuster u gui i nasao par zanimljivih fajlova

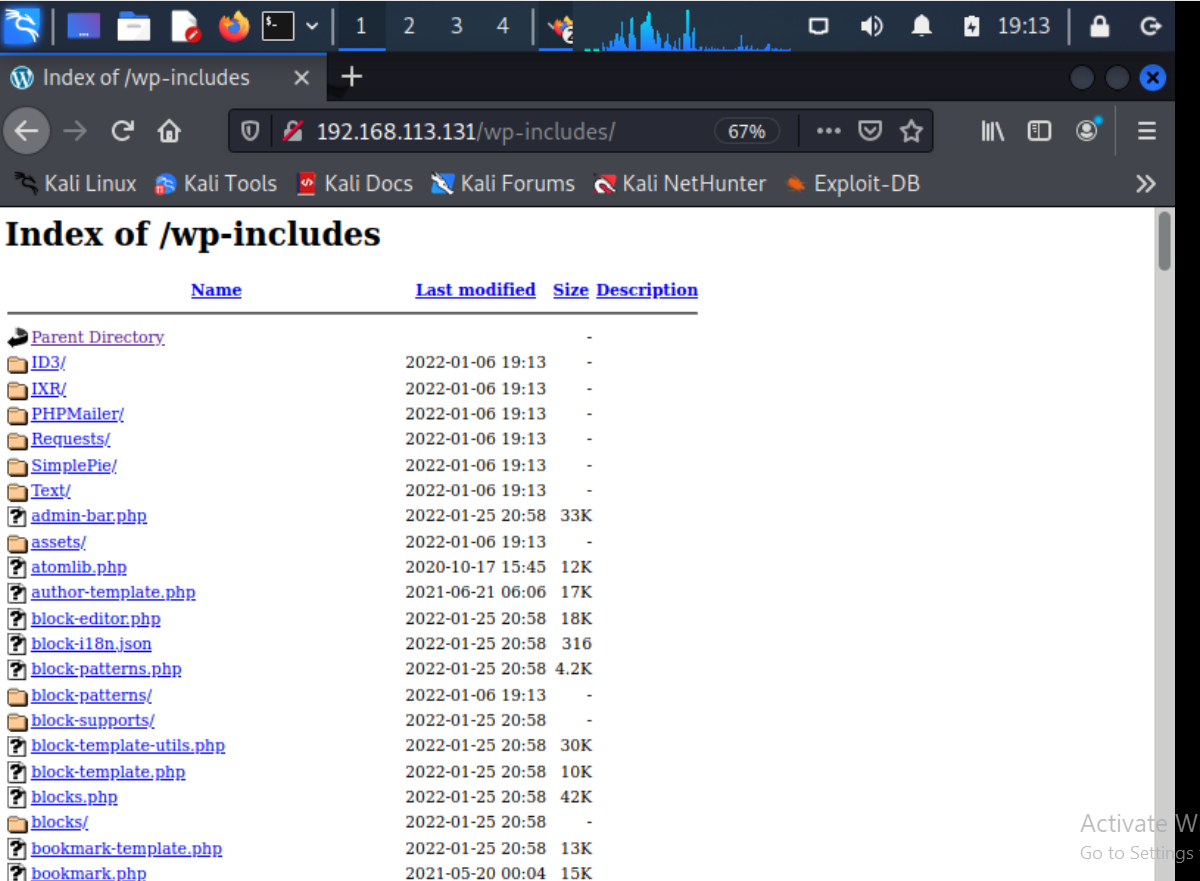


Takode sam pokrenuo i gobuster



Ubrzo dobijam



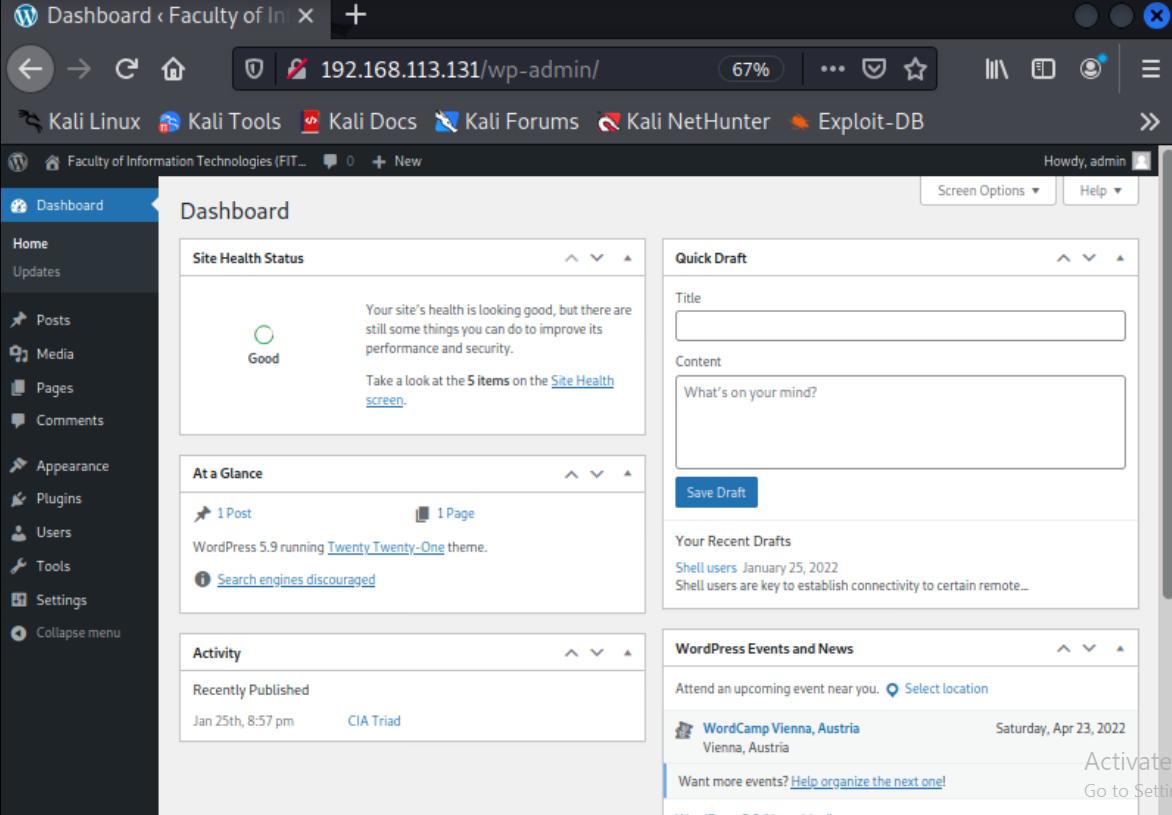


Slabost

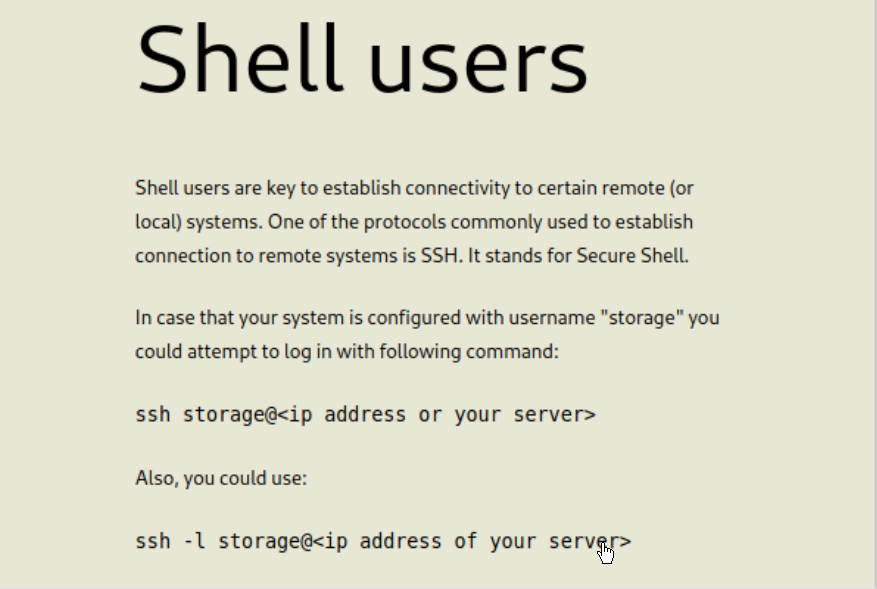
Fajlovi kao /wp-includes i /info/info.php ne bi trebali biti vidjljivi.

Na /wp-login.php

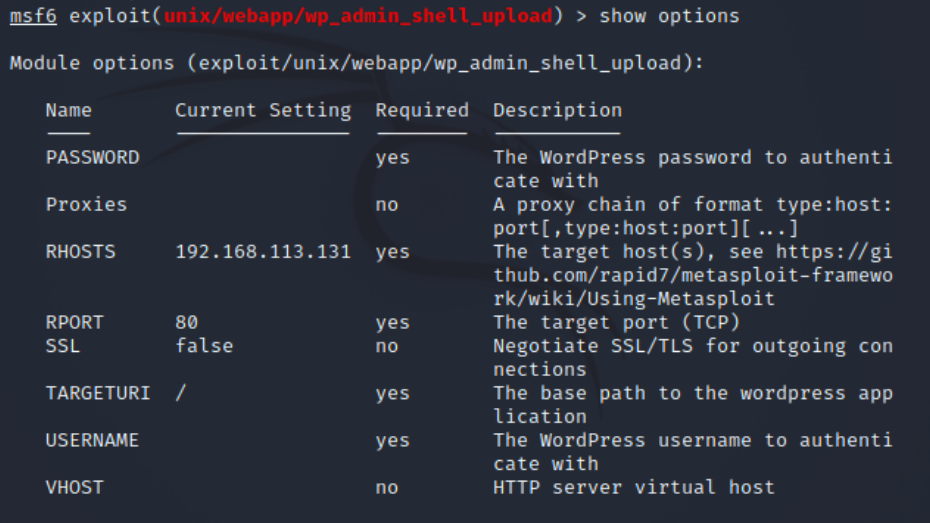
Logiram se sa podacima pronadenim



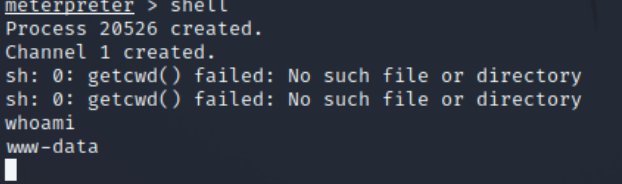
Pronalazim draf sa hintom



Pokrecem metasploit(msfconsole) i preko searcha trazim exploit za wp admina shell

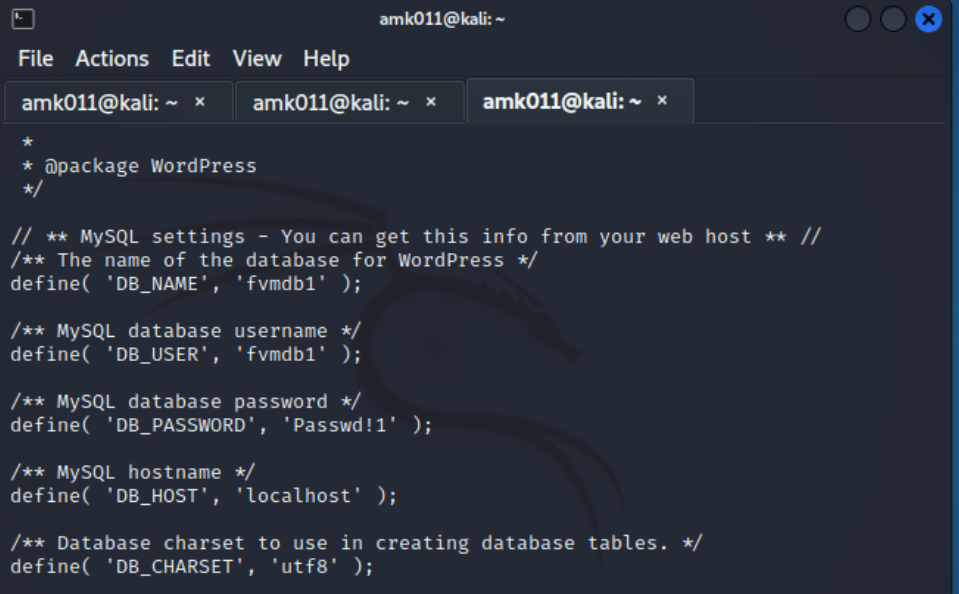


Setam password i usernam i pokrecem ga

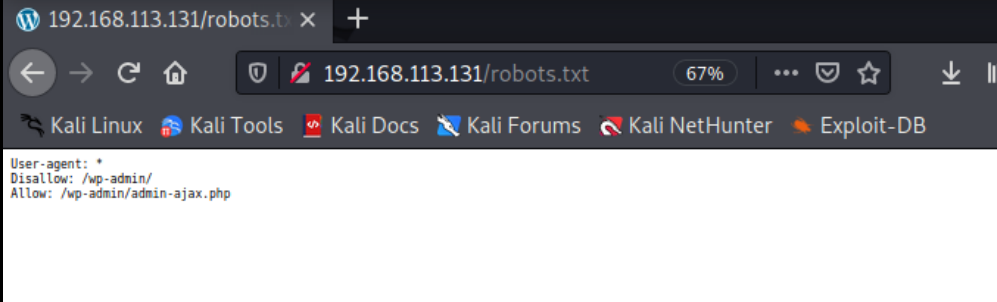


Nalazim se u www-data i pokrecem shell

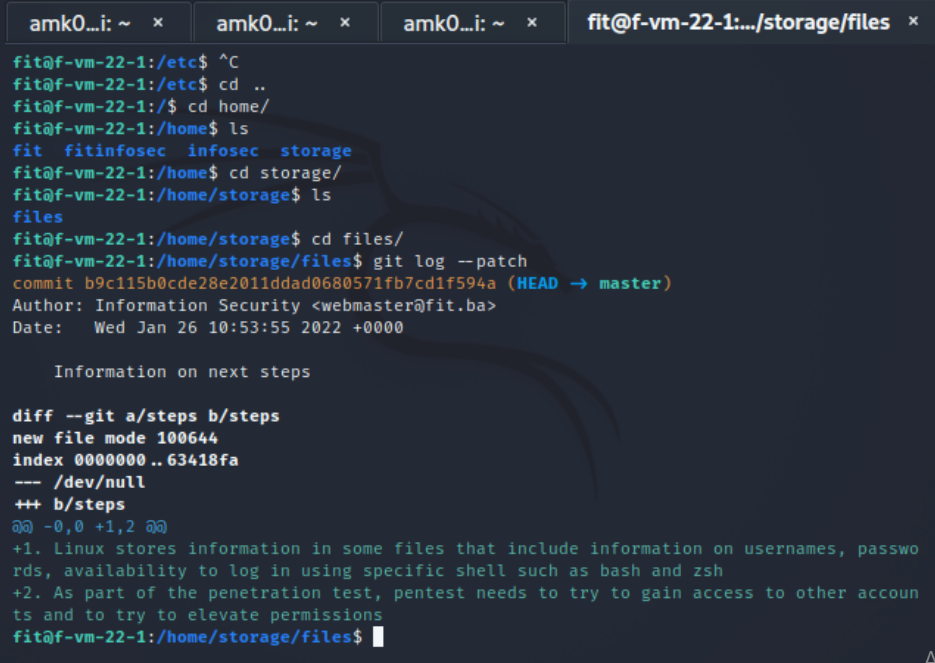
Sada navigiram u sistemu i pronalazim wp-config.php gdje pronalazim username i password od mysql servisa



robots.txt je vulnerabilit



Hint za git



Hashcat za infosec

