

Name of the Company: MentorrBuddy

Project: Mr Robot 1

Guide Name: Gurvansh singh

Teammates : Vigneshini

Md Mahin Uddin

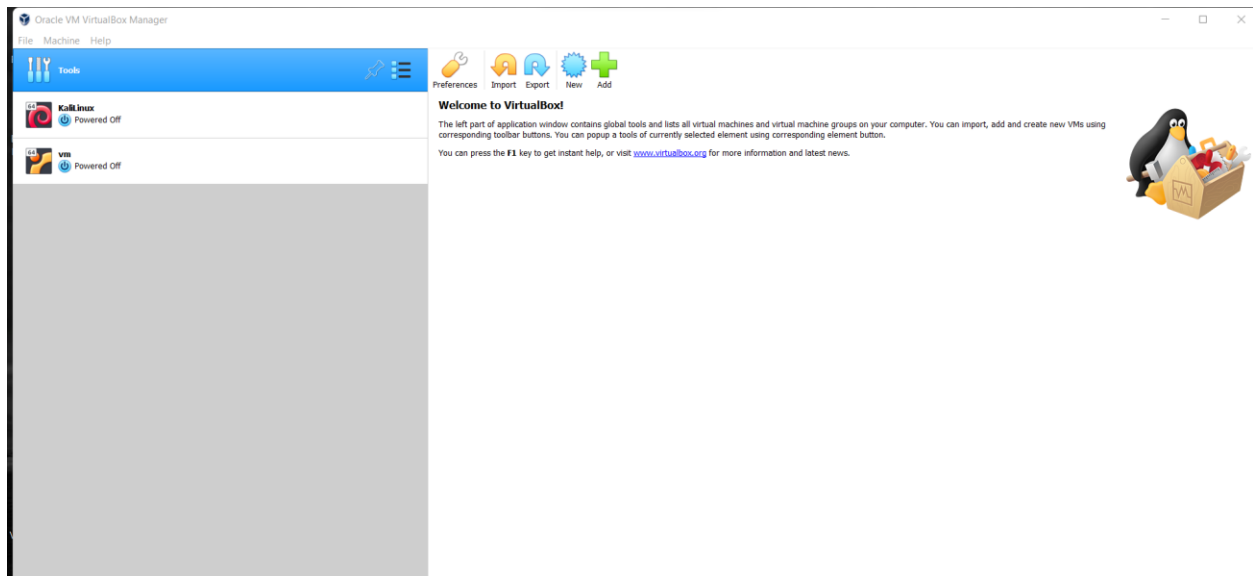
Thilothamai

About Mr-Robot: 1

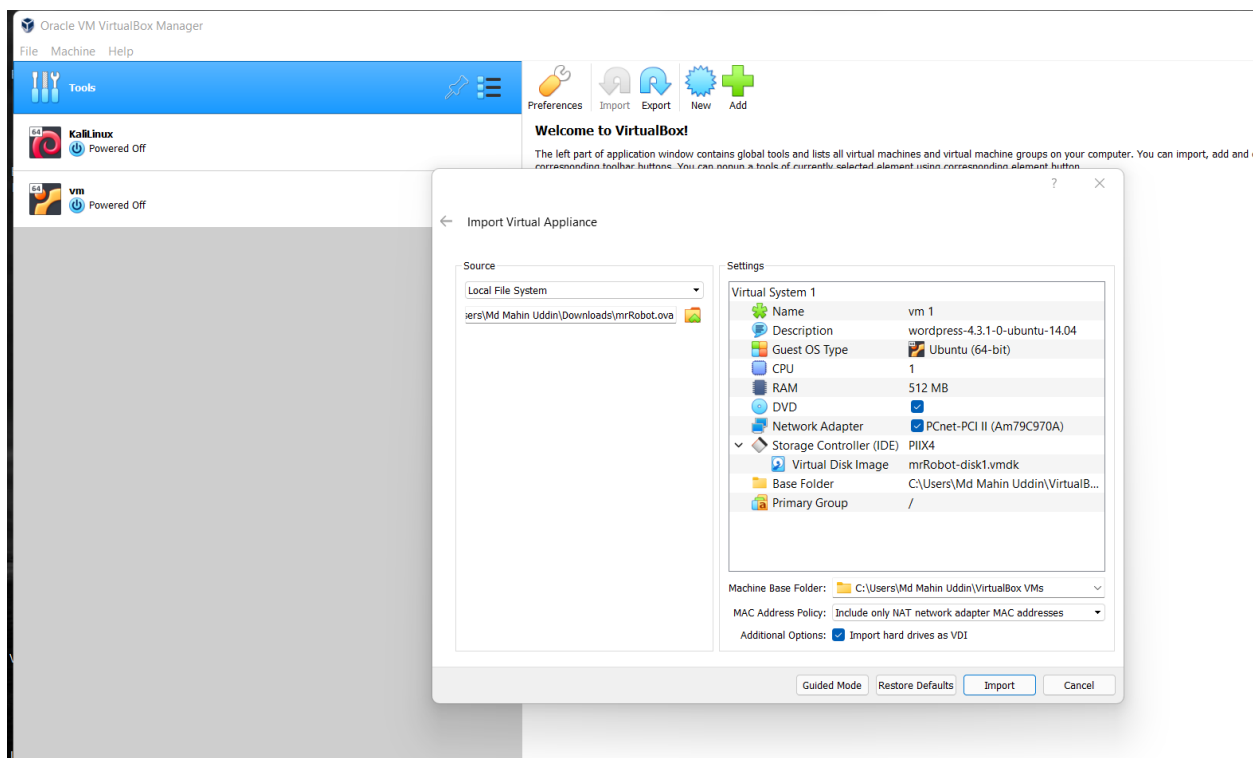
Based on the show, Mr. Robot.

This VM has three keys hidden in different locations. Your goal is to find all three. Each key is progressively difficult to find.

The VM isn't too difficult. There isn't any advanced exploitation or reverse engineering. The level is considered beginner-intermediate.



First of all we need to import this ova file and start this and then we have to start this like this



Now,

We need to run after start and let's see what will happen



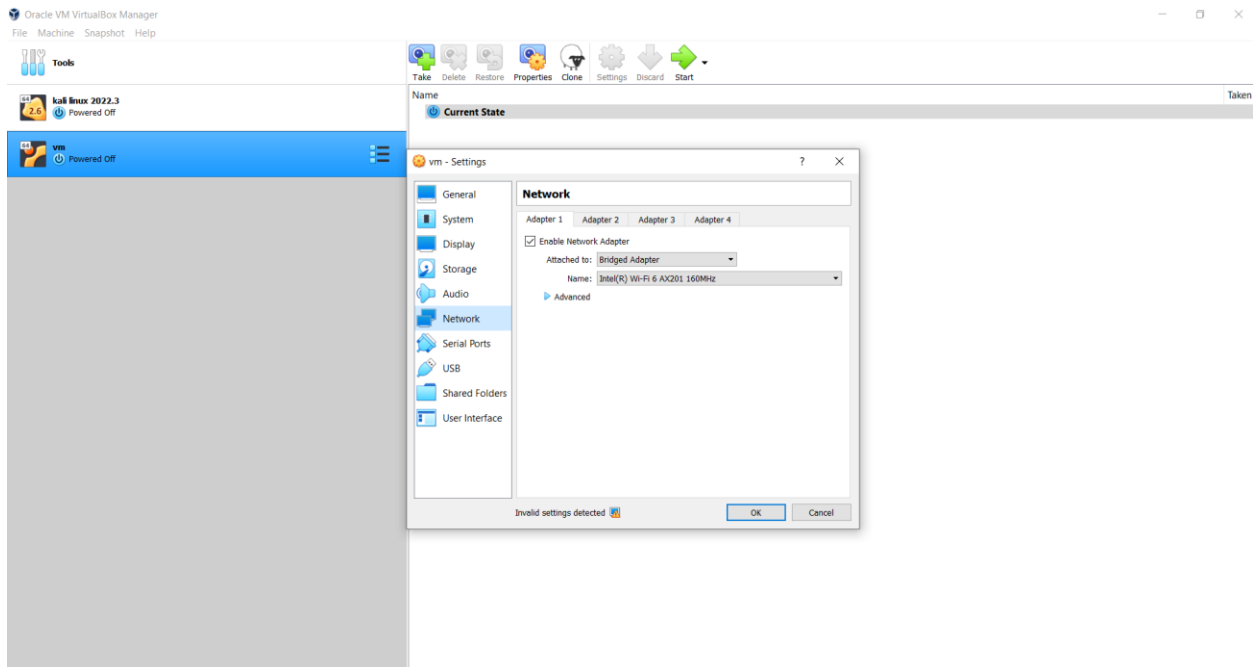
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.

The highlighted entry will be booted automatically in 2 seconds.



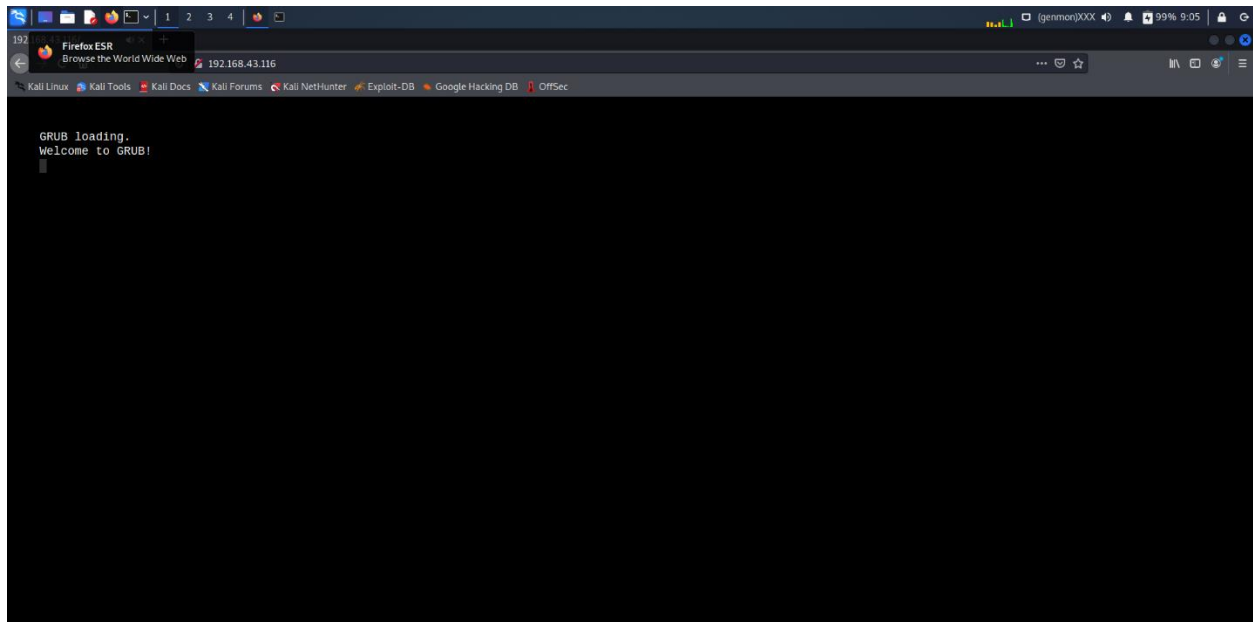
After that we need to change our internet connection to Bridged Adapter for fully scan the network

Under the Bridged Adapter, our virtual machines behave as any other computer on the network where the hosting system resides; it **bridges the virtual and physical networks**. ... The Bridged Adapter connects through the host to whatever is your default network device that allocates IP addresses for your physical network....

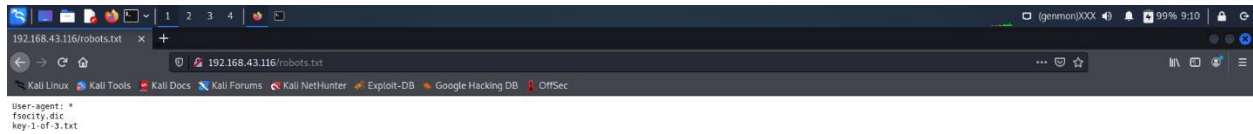


And it's time to scan the networks to use "ifconfig" command

The "ifconfig" command is used for **displaying current network configuration information**, setting up an ip address, netmask, or broadcast address to a network interface, creating an alias for the network interface, setting up hardware address, and enable or disable network interfaces...

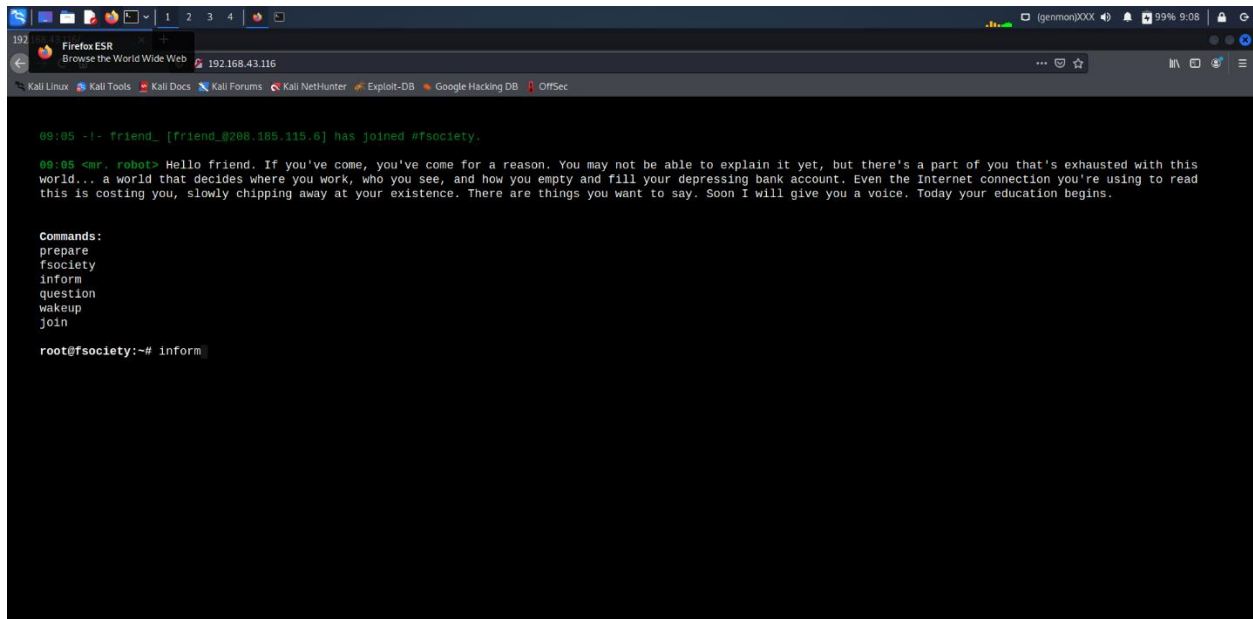


As we can see below, we have a hit for robots.txt.....



And now whenever we scan our ip address we can see this type of window....(below).

/



```
09:05 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

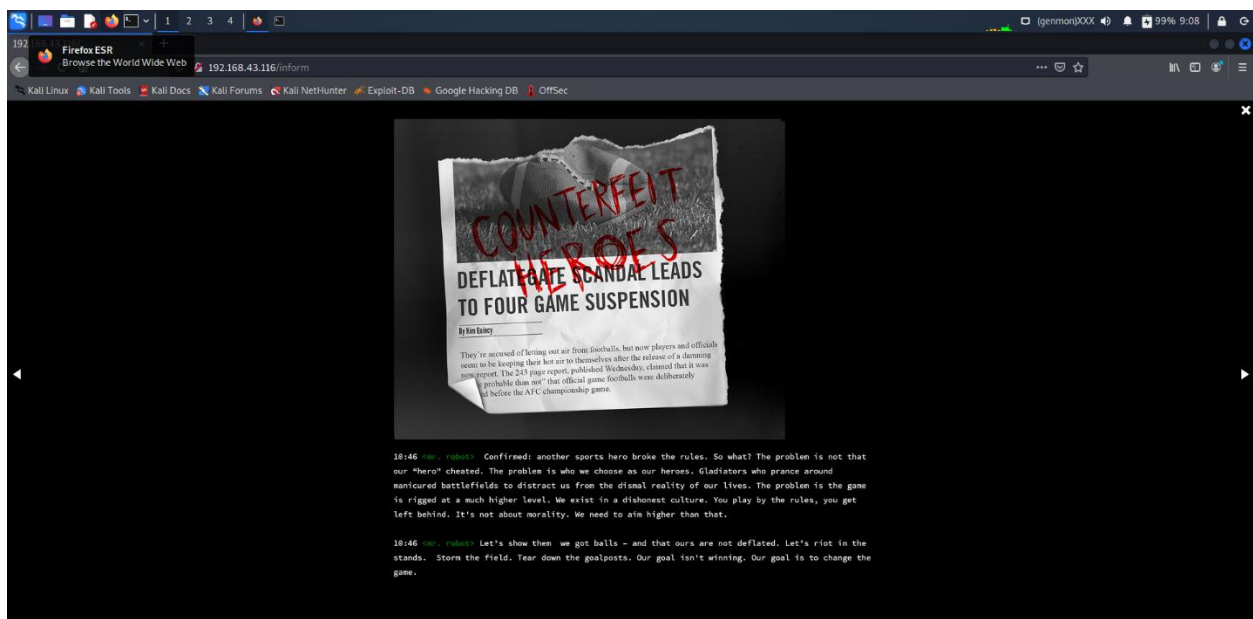
09:05 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.

Commands:
prepare
fsociety
inform
question
wakeup
join

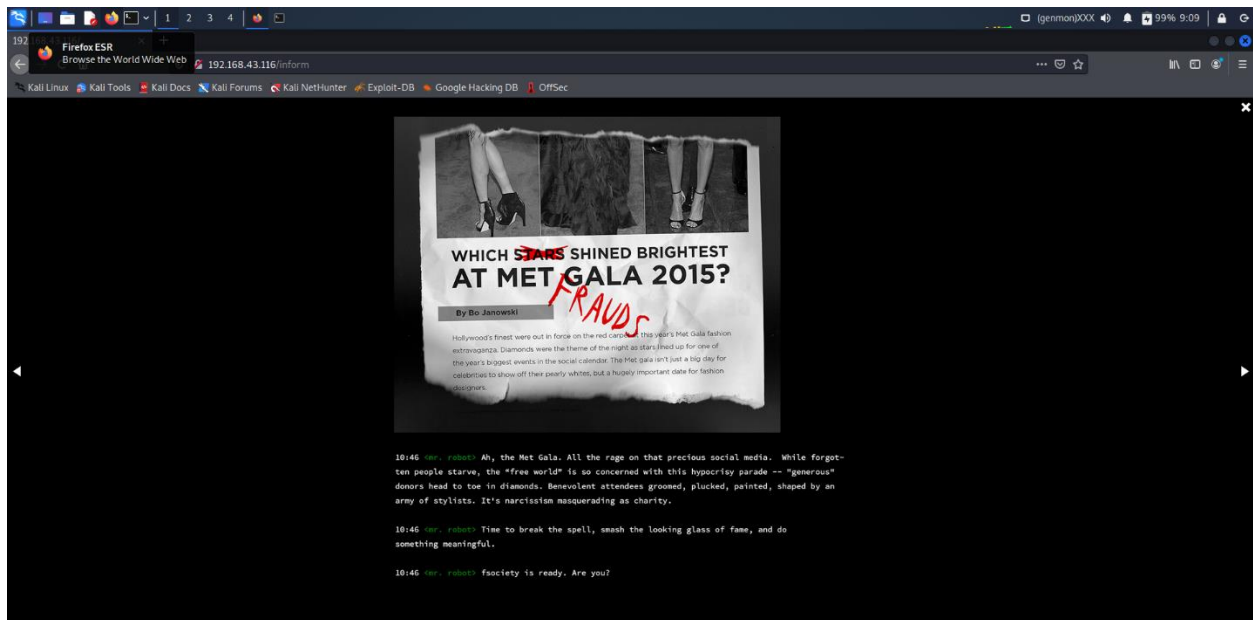
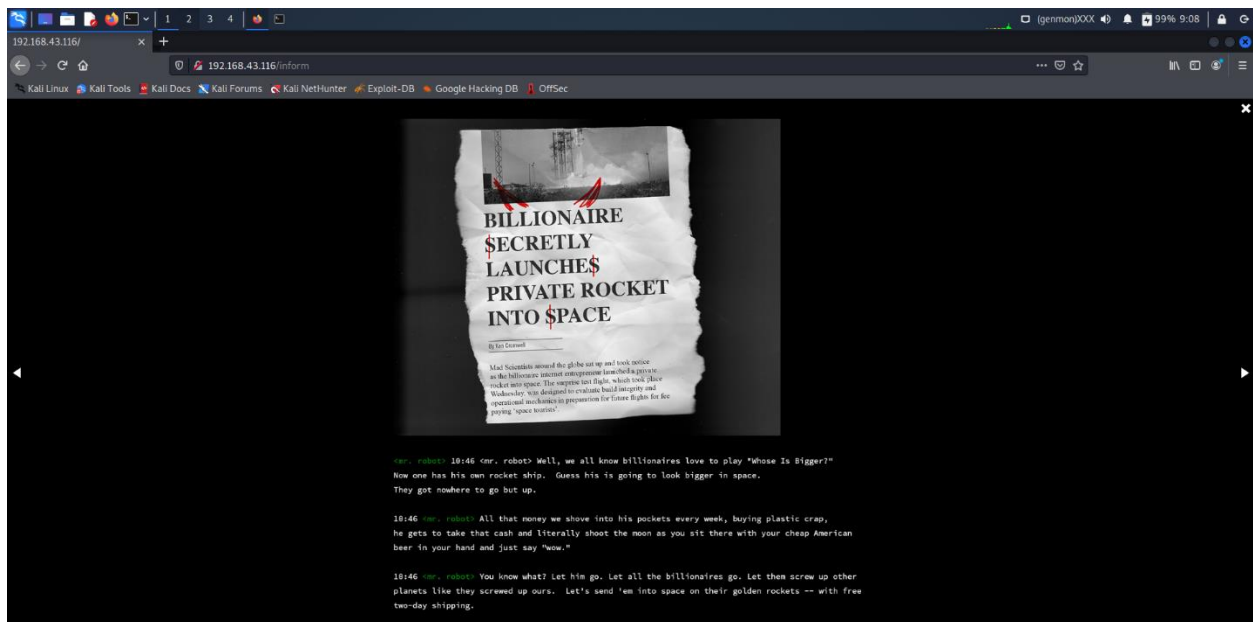
root@fsociety:~# inform
```

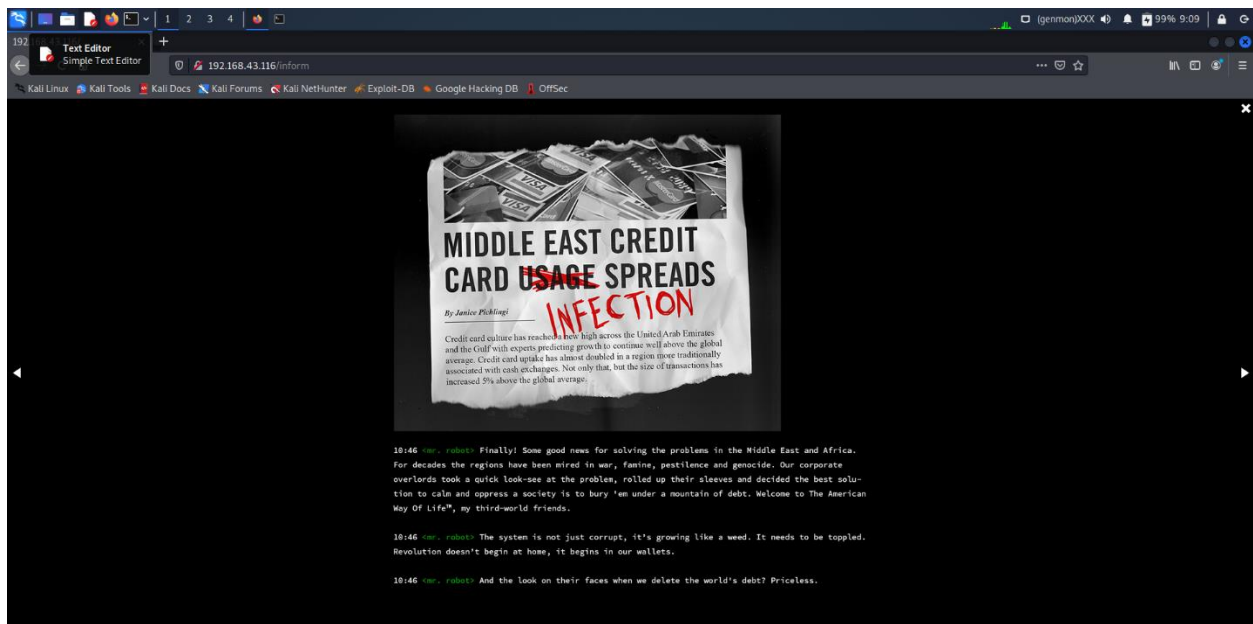
Now we will use the “inform” one we will write it on our kali’s Browser after we write our ip address like this “192.168.43.116/inform”

Like below



And then goes on like this.....





Boom!!!! We got our first key key-1-of-3.txt.....

```

root@kali: ~
File Actions Edit View Help
root@kali: ~ * root@kali: ~ *
inet6 2489:4872:710:2502:a00:27ff:fc9:1c0d prefixlen 64 scopeid 0<global>
inet6 2489:4872:710:2502:b983:ecb4:712b:f3f9 prefixlen 64 scopeid 0<global>
ether 8b:80:27:c9:1c:00 txqueuelen 1000 (Ethernet)
RX packets 21 bytes 2406 (2.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4918 bytes 295746 (288.8 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

[root@kali:~]#
# wget 192.168.43.116/fsociety.dic
--2022-01-27 18:06:20-- http://192.168.43.116/fsociety.dic
Connecting to 192.168.43.116:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: 'fsociety.dic.1'

fsociety.dic.1 100%[=====] 6.91M 30.0MB/s in 0.2s

2022-01-27 18:06:20 (30.8 MB/s) - 'fsociety.dic.1' saved [7245381/7245381]

[root@kali:~]#
# wget 192.168.43.116/key-1-of-3.txt
--2022-01-27 18:06:54-- http://192.168.43.116/key-1-of-3.txt
Connecting to 192.168.43.116:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33 [text/plain]
Saving to: 'key-1-of-3.txt'

key-1-of-3.txt 100%[=====] 33 --KB/s in 0s

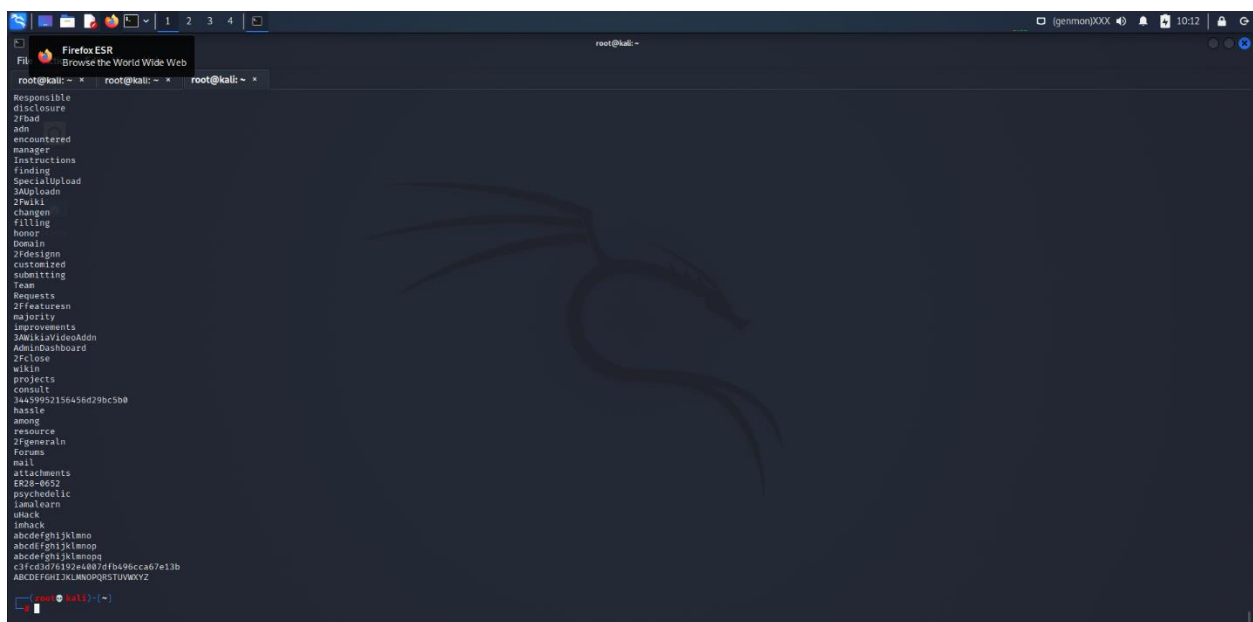
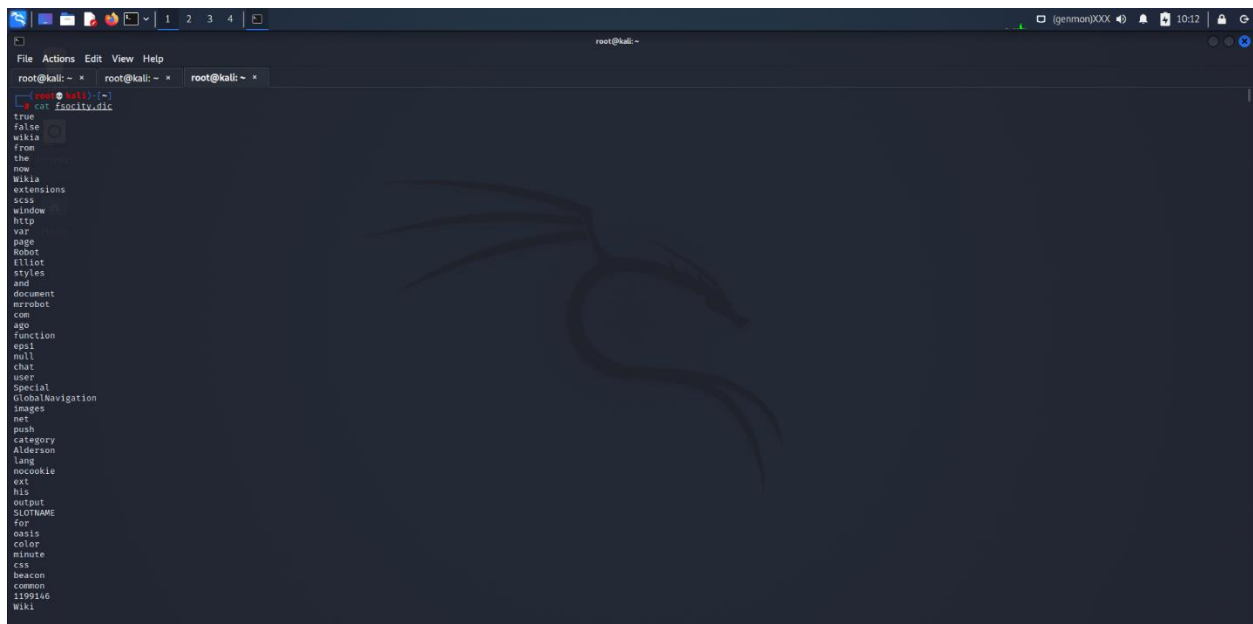
2022-01-27 18:06:54 (3.55 MB/s) - 'key-1-of-3.txt' saved [33/33]

[root@kali:~]#
# cat key-1-of-3.txt
073403cd8a58a1f884943455fb0724b9
[root@kali:~]#

```

Now we need to gather the information that's why we used "cat fsociety.dic

Fsociety is a free and open-source tool available on GitHub which is used as an information-gathering tool. Fsociety is used to scanning websites for information gathering and finding vulnerabilities in websites and web apps.....

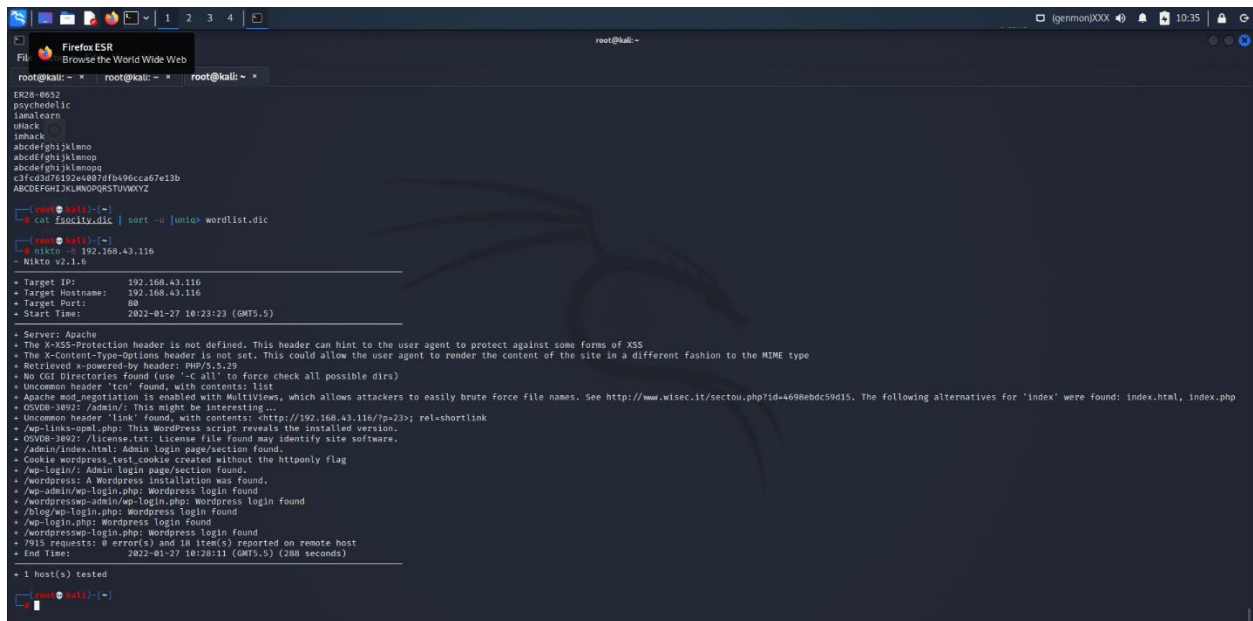


Now we want to scan a server IP so we need to type this command, it will take some time and show us some vulnerability if exists.

Command: **nikto -h serverIp .**

Example: **nikto-h 192.168.43.116**

Here -h means the **host**.



```
root@kali: ~  
ER28-0652  
psychodalic  
sm3learn  
uhack  
jmhack  
abcdefghijklmno  
abcdeffghijklmno  
abcdeffghijklmno  
c3fc03d76192e4807dfb96cca67e13b  
ABKDEFGHIJKLNMOPQRSTUVMXYZ  
  
root@kali:~# cat /usr/share/wordlists/wordlist.txt | sort -u | uniq -u | xargs curl -s -o /dev/null -w '%s\n' http://192.168.43.116/  
- Nikto v2.1.5  
  
+ Target IP: 192.168.43.116  
+ Target Hostname: 192.168.43.116  
+ Target Port: 80  
+ Start Time: 2022-01-27 10:23:23 (GMT+5)  
  
+ Server: Apache  
+ The X-SS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.  
+ Retrieved x-powered-by header: PHP/5.5.29  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Uncommon header 'tcn' found, with contents: list  
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html, index.php  
+ OSVDB-3992 /Admin/: This might be interesting...  
+ Uncommon header 'link' found, with contents: <http://192.168.43.116/?p=23>; rel=shortlink  
+ /wp-links-opml.php: This WordPress script reveals the installed version.  
+ OSVDB-3992 /license.txt: License file found may identify site software.  
+ /admin/index.html: Admin login page/section found.  
+ Cookie wordpress_test_cookie created without the httponly flag  
+ /wp-login/: Admin login page/section found.  
+ /wordpress: A Wordpress installation was found.  
+ /wp-admin/wp-login.php: Wordpress login found  
+ /wordpress/wp-admin/wp-login.php: Wordpress login found  
+ /blog/wp-login.php: Wordpress login found  
+ /wp-login.php: Wordpress login found  
+ /wordpress/wp-login.php: Wordpress login found  
+ 7915 requests: 0 error(s) and 18 item(s) reported on remote host  
+ End Time: 2022-01-27 10:28:11 (GMT+5) (288 seconds)  
  
+ 1 host(s) tested  
  
root@kali:~#
```

We got our informations and target ports.....

Now its time to install our Wpscan

WPScan is a **command-line WordPress vulnerability scanner** that can be used to scan WordPress vulnerabilities. It comes pre-installed on the following penetration testing Linux distributions...

```
root@kali: ~  
wpscan --url http://wordpress.org --api-token QnaghkRusf81Y9r18fPC8G07npkanytrFasAeggs  
  
WordPress Security Scanner by the WPScan Team  
Version 3.8.20  
Sponsored by Automattic - https://automattic.com/  
@WPScan, @ethicalhack3r, @erwan_l_r, @l33t4r  
  
[-] URL: http://wordpress.org/ [198.143.164.252]  
[-] Effective URL: https://wordpress.org/  
[-] Started: Sun Jan 30 12:18:24 2022  
  
Interesting Finding(s):  
[-] Headers  
Interesting Entries:  
- server: nginx  
- x-olef: 0  
- x-nc: HIT ord 2  
Found By: Headers (Passive Detection)  
Confidence: 100%  
  
[-] This site has 'Must Use Plugins': http://wordpress.org/wp-content/mu-plugins/  
Found By: URLs in Homepage (Passive Detection)  
Confidence: 100%  
Confirmed By: Direct Access (Aggressive Detection), 88% confidence  
Reference: http://codex.wordpress.org/Must_Use_Plugins  
  
Fingerprinting the version - Time: 00:01:14  
[-] The WordPress version could not be detected.  
  
[-] WordPress theme in use: pub  
Location: http://wordpress.org/wp-content/themes/pub/  
Style URL: http://wordpress.org/wp-content/themes/pub/style.css  
Found By: Urls in 404 Page (Passive Detection)  
The version could not be determined.  
  
[-] Enumerating All Plugins (via Passive Methods)  
[-] Checking Plugin Versions (via Passive and Aggressive Methods)
```

```
root@kali: ~  
wpscan --url http://wordpress.org --api-token QnaghkRusf81Y9r18fPC8G07npkanytrFasAeggs  
  
[-] Title: Jetpack < 9.8 - Carousel Module Non-Published Page/Post Attachment Comment Leak  
Fixed in: 9.8  
References:  
- https://wpscan.com/vulnerability/0a8a51c-49d1-4bce-57eb-e365afid8f33  
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26314  
- https://jetpack.com/2021/06/01/jetpack-9-8-engage-your-audience-with-wordpress-stories/  
- https://plugins.trac.wordpress.org/changeset/2541817/jetpack  
The version could not be determined.  
  
[-] Stream  
Location: http://wordpress.org/wp-content/plugins/stream/  
Last Updated: 2021-10-18T12:25:00-0002  
[-] The version is out of date, the latest version is 3.8.2  
Found By: Comment (Passive Detection)  
[-] 1 vulnerability identified:  
[-] Title: Stream < 3.8.2 - Admin+ SQL Injection  
Fixed in: 3.8.2  
References:  
- https://wpscan.com/vulnerability/b9d4f2ad-2f12-4822-817d-982a016af85d  
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24772  
- https://plugins.trac.wordpress.org/changeset/2615811/stream  
Version: 3.6.2 (48% confidence)  
Found By: Comment (Passive Detection)  
- https://wordpress.org/, Match: 'Stream WordPress user activity plugin v3.6.2'  
  
[-] Enumerating Config Backups (via Passive and Aggressive Methods)  
Checking Config Backups - Time: 00:00:00  
[-] No Config Backups Found.  
  
[-] WPScan DB API OK  
Plan: free  
Requests Done (during the scan): 0  
Requests Remaining: 10  
  
[-] Finished: Sun Jan 30 12:19:53 2022  
[-] Requests Done: 1246  
[-] Cached Requests: 58  
[-] Data Sent: 277.462 KB  
[-] Data Received: 331.633 KB  
[-] Memory used: 237.375 MB  
[-] Elapsed time: 00:01:28  
  
root@kali: ~
```