**WRITE UP TRYHACKME : VULNVERSITY**

**CYBER SECURITY**

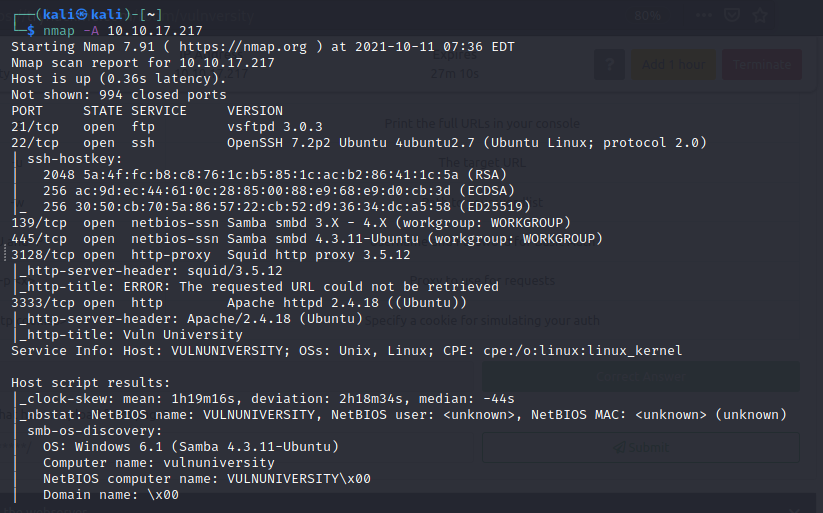
**REZKA NORHAFIZAH**

**DEPLOY THE MACHINE**

*Connect to vpn : sudo openvpn rezzz.ovpn*

**RECONNAISSANCE**

* Scan the box, how many ports are open?



Saya jalankan dengan perintah **nmap -A 10.10.17.217**

**Answer : 6**

* What version of the squid proxy is running on the machine?

Dari gambar sebelumnya dapat diketahui bahwa squid http proxy yang digunakan adalah versi 3.5.12 dan running pada port 3128.

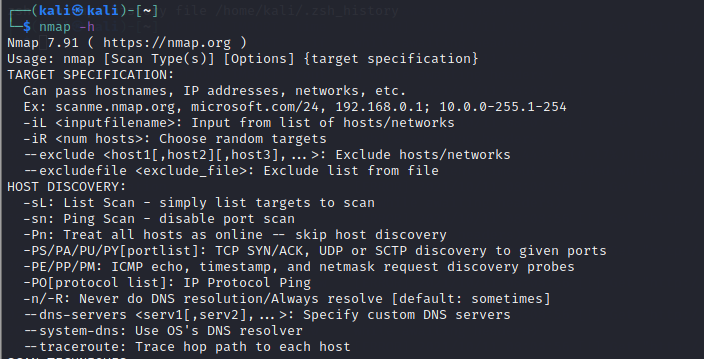
**Answer : 3.5.12**

* How many ports will nmap scan if the flag -p-400 was used?

**Answer : 400**

* Using the nmap flag **-n** what will it not resolve?

Saya ketik perintah nmap -h :



**Answer : DNS**

* What is the most likely operating system this machine is running?

Dari gambar 1 dapat dilihat bahwa OS yang digunakan adalah Ubuntu.

**Answer : Ubuntu**

* What port is the web server running on?

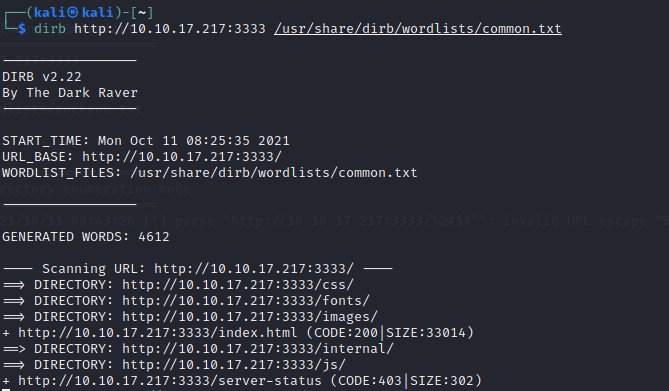
Dari gambar 1 terlihat Apache2 running pada port 3333.

**Answer : 3333**

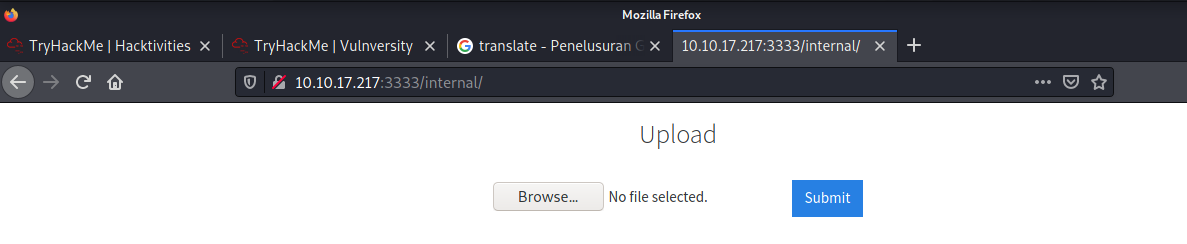
**LOCATING DIRECTORIES USING GOBUSTER**

* What is the directory that has an upload form page?

Saya menggunakan dirb untuk menscan direktori yang terbuka dengan perintah **dirb** [**http://10.10.10.17.217:3333**](http://10.10.10.17.217:3333) **/usr/share/wordlist/rockyou.txt**



Dan didapat internal sebagai direktori yang mengandung form upload :

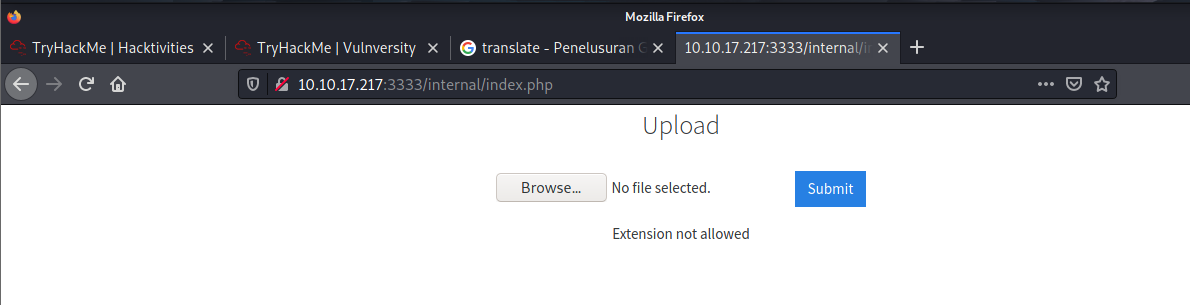


**Answer : /internal/**

**COMPROMISE THE WEBSERVER**

* Try upload a few file types to the server, what common extension seems to be blocked?

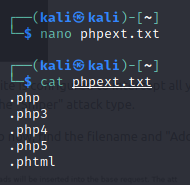
Karena hint terdiri dari 3 huruf, maka saya coba memasukkan file berekstensi php karena ekstensi tersebut yang paling sering digunakan. Ternyata berhasil :



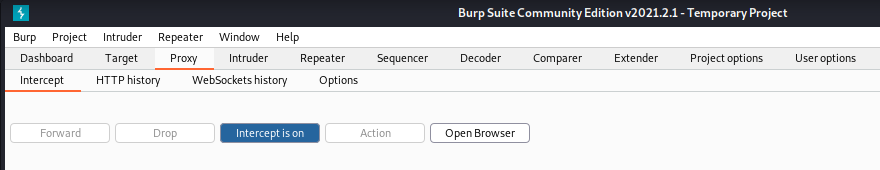
**Answer : .php**

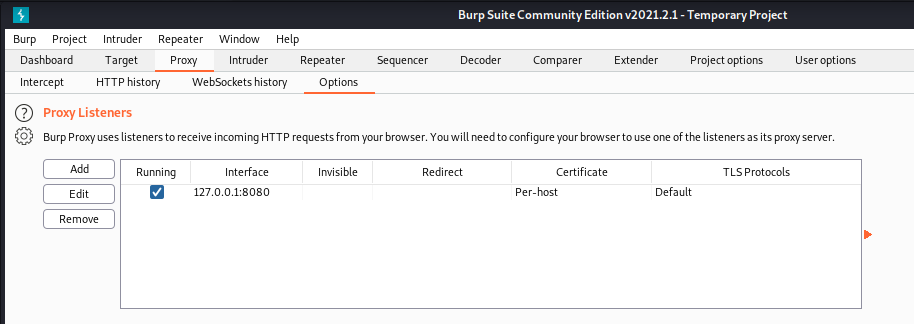
* Run this attack, what extension is allowed?

Sesuai yang diinstruksikan oleh soal saya membuat file phpext.txt dengan isi :

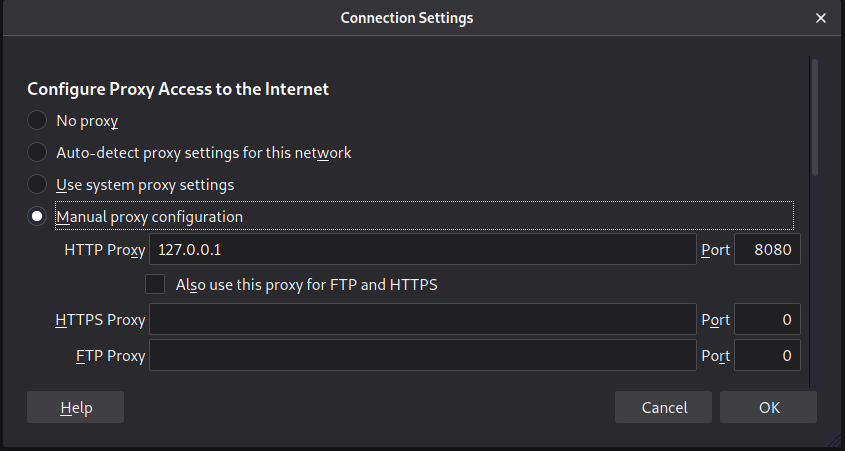


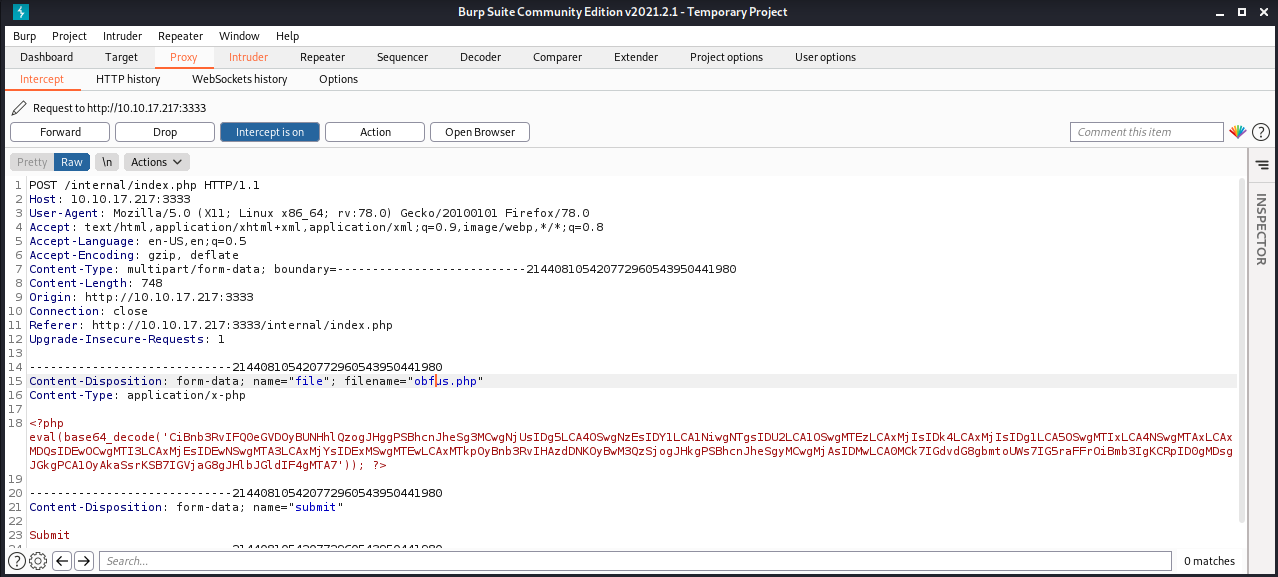
Lalu, gunakan Burp Suite untuk mengetahui file ekstensi apa yang diperbolehkan untuk diupload. Pertama, buka Burp Suite di Kali dan pastikan interceptnya on :



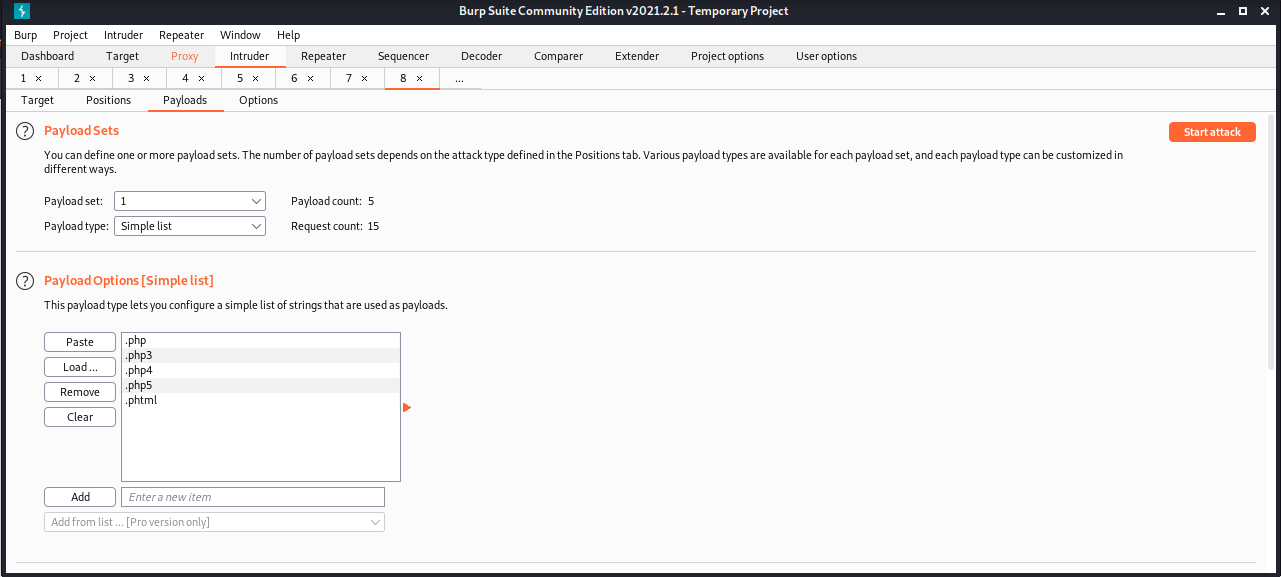
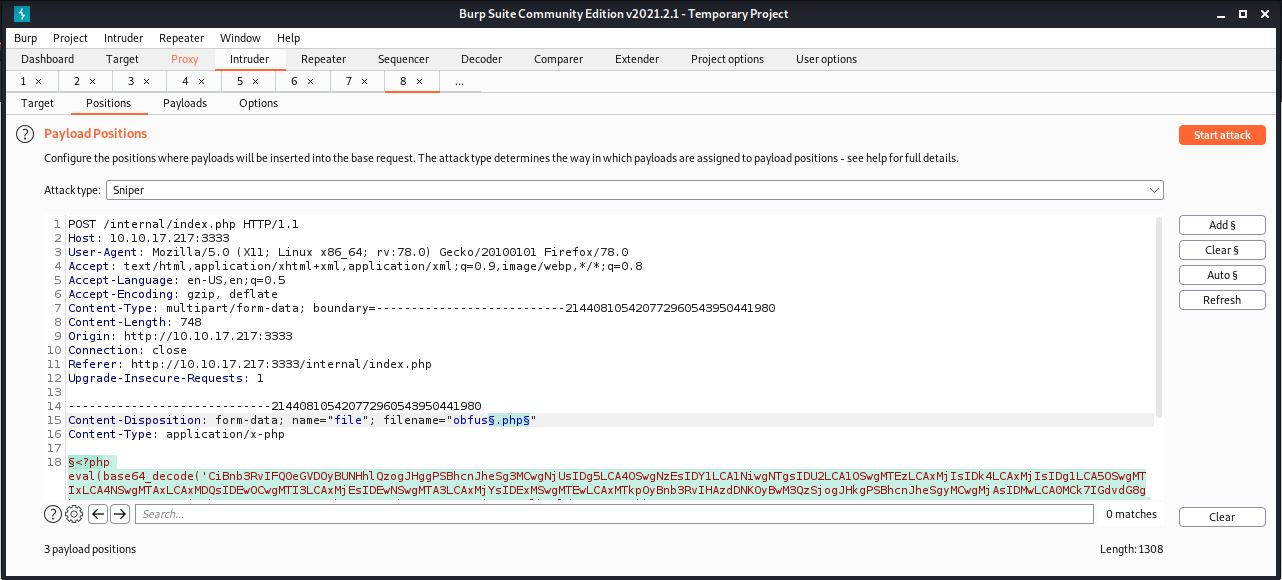


Ketik ip di atas pada tab preferences > general > network settings > settings

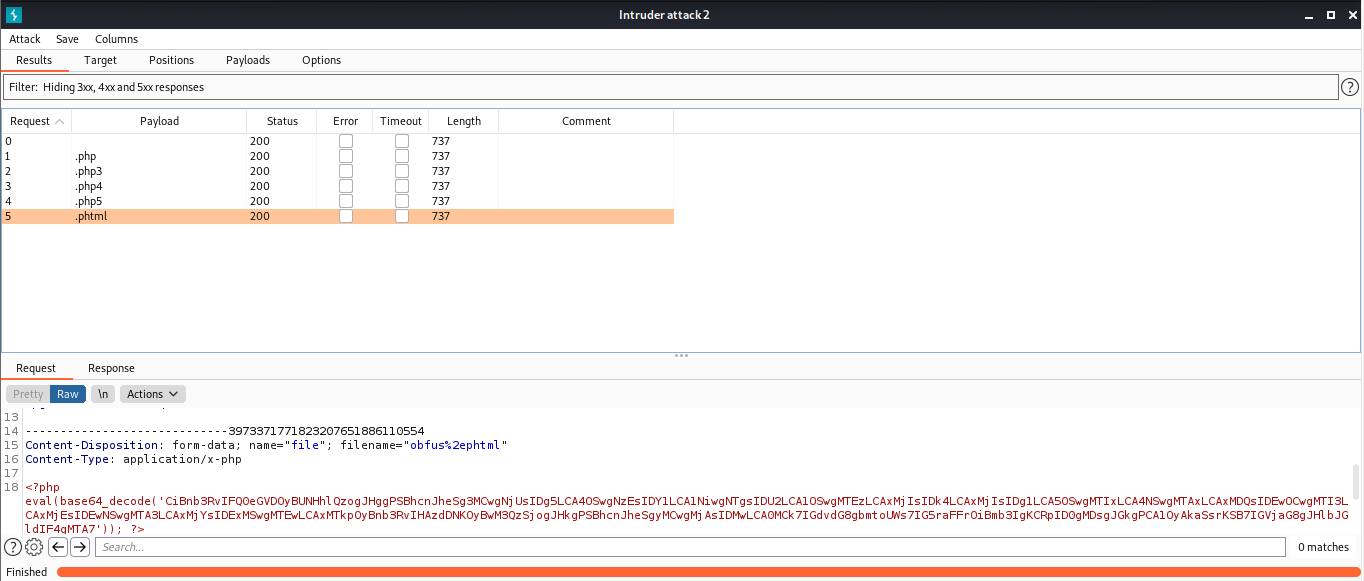


Setelah itu, coba upload file php dan Burp Suite akan secara otomatis menangkap request yang kita lakukan. Setelah itu, forward ke intruder dengan mengklik Ctrl+i

Setelah itu pada intruder pergi ke tab payloads dan masukkan file phpext.txt tadi. Lalu pada tab positions klik tombol Add $ seperti pada gambar :

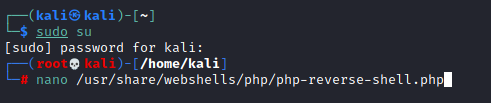
Selanjutnya, klik start attack dan didapat :

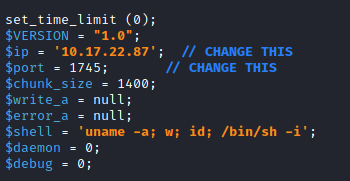


**Answer : .phtml**

* What is the name of the user who manages the webserver?

Pertama-tama saya akan menanam shell ke web yang sudah diberikan tadi. File php shell di Kali berada di /usr/share/webshells/php/php-reverse-shell.php. Buka file tersebut dan ganti ip sesuai ip host dan port seperti berikut :

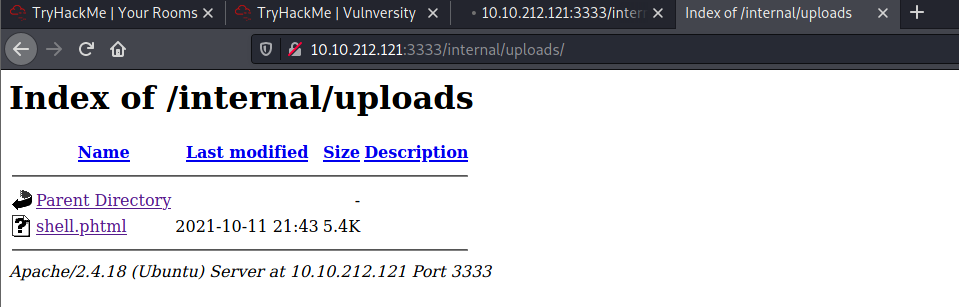




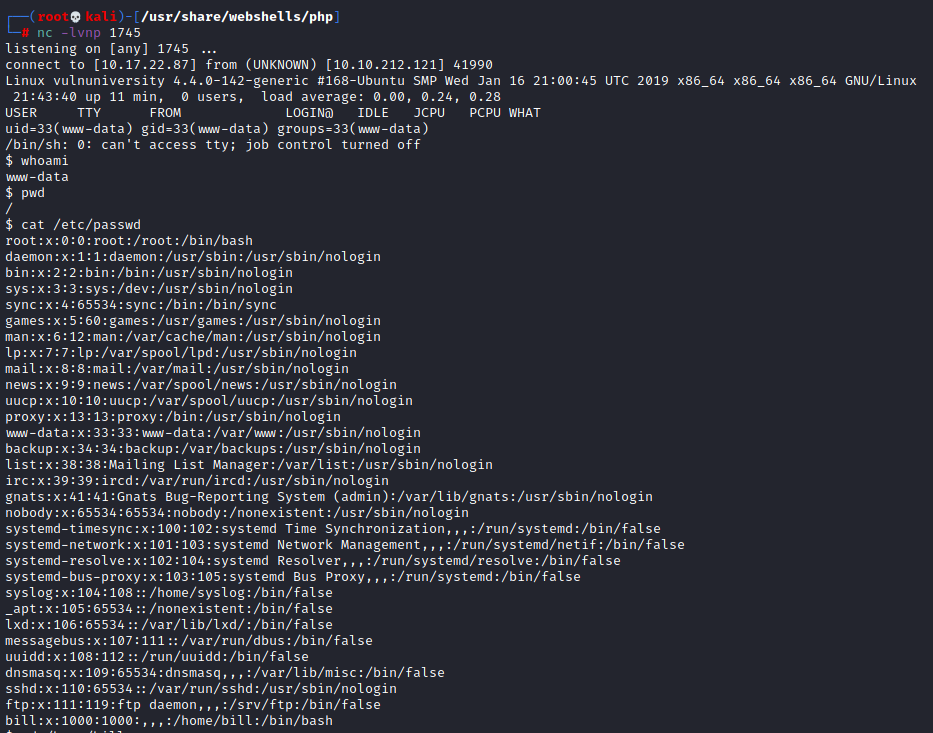
Kemudian karena ekstensi file yang diperbolehkan hanya phtml maka saya ubah ekstensi nya menjadi phtml :

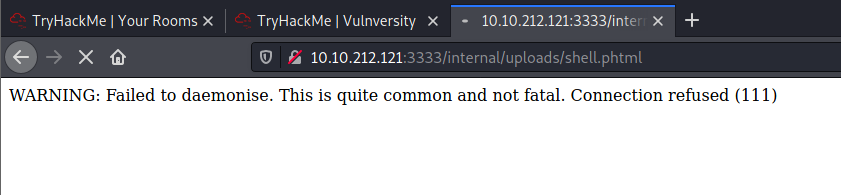


Setelah itu upload dan lihat apakah shell nya sdh berhasil diupload atau tidak dengan melihat ke <http://10.10.212.121:3333/internal/uploads> :

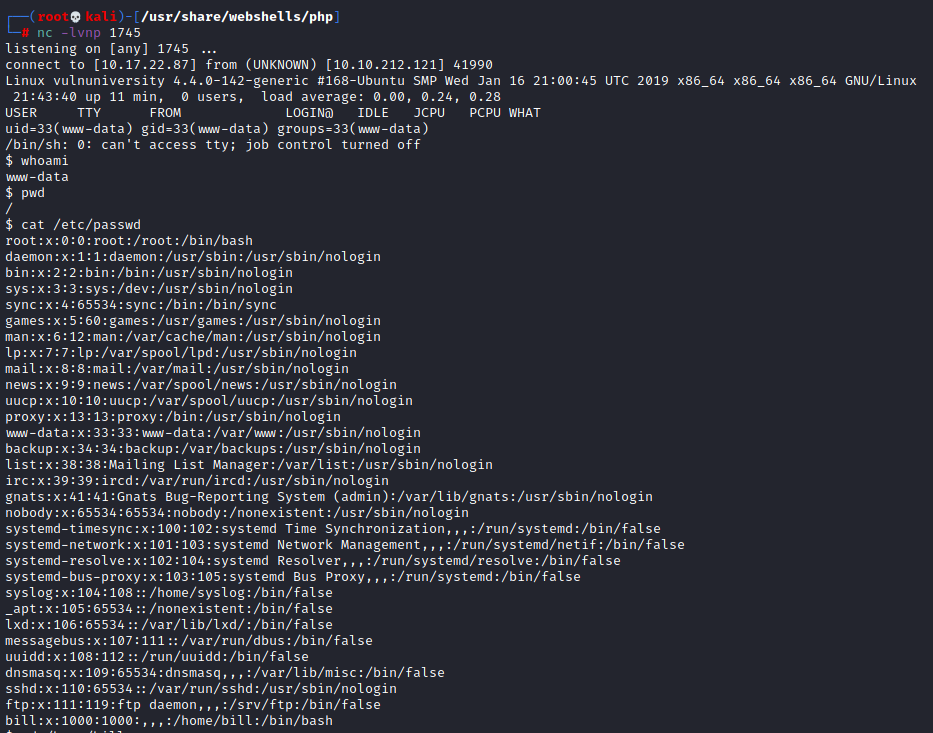


Jika sudah berhasil tinggal jalankan nc dan masukkan sesuai port yang sudah diganti tadi kemudian eksekusi shell lewat web :





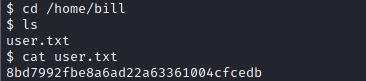
Jika sudah berhasil masuk, cari user apa yang ada dalam machine tersebut dengan mengetik command :



**Answer : bill**

* What is the user flag?

Masuk ke folder /home/bill dan ternyata ada file user.txt yang berisi flag :



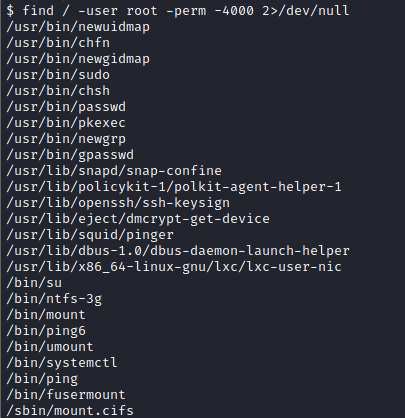
**Answer : 8bd7992fbe8a6ad22a63361004cfcedb**

**PRIVILEGE ESCALATION**

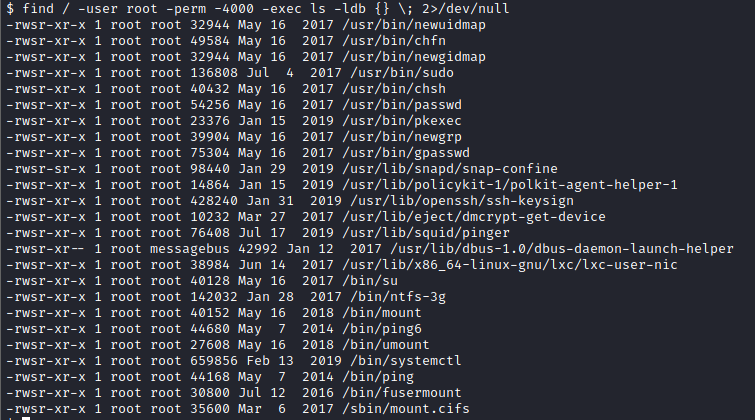
* On the system, search for all SUID files. What file stands out?

*Hint : Use the command: find / -user root -perm -4000 -exec ls -ldb {} \;*

Cari file dengan kepemilikan root dan permission SUID :

**

Atau bisa juga dengan :

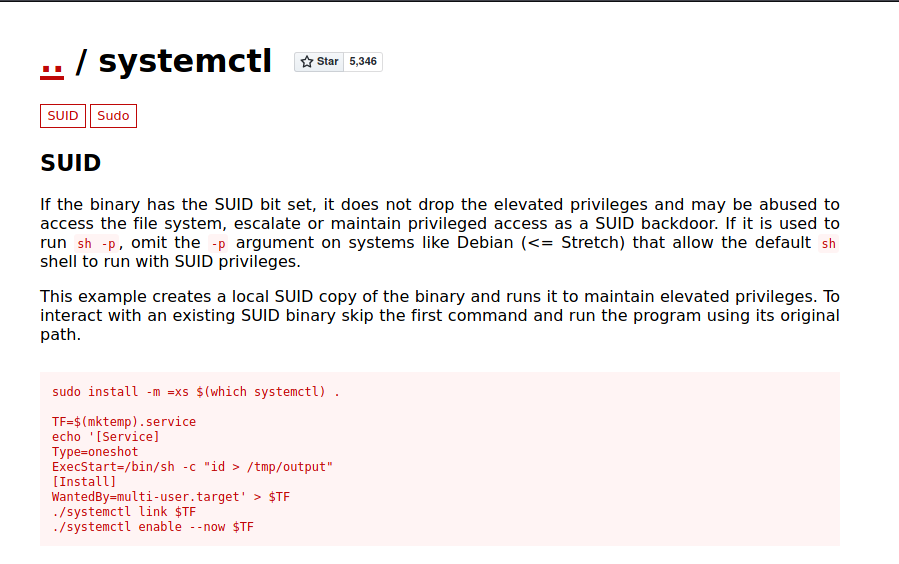


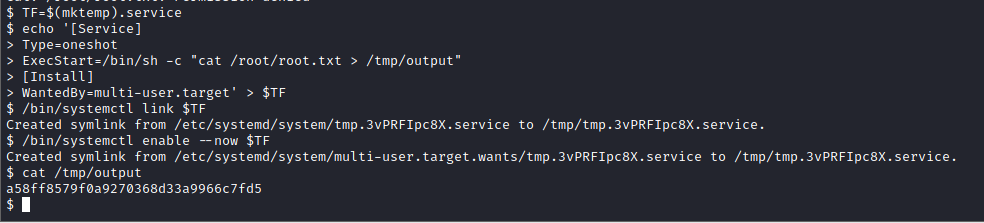
**Answer : /bin/systemctl**

* Its challenge time! We have guided you through this far, are you able to exploit this system further to escalate your privileges and get the final answer? Become root and get the last flag (/root/root.txt)

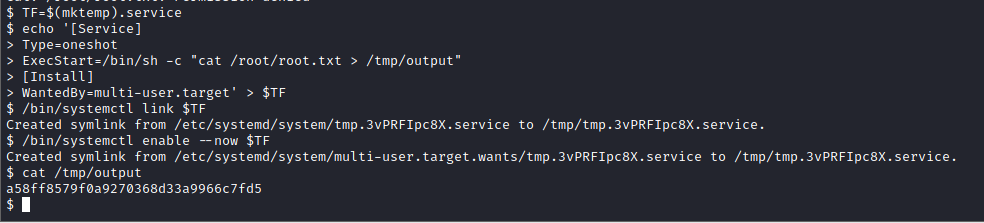
*Hint : /bin/systemctl*

Setelah ditemukan file /bin/systemctl tadi saya menemukan di gtfobins cara untuk mendapat root yaitu dengan cara :

**

**

Perintah di atas berguna untuk kita mengubah id root ke /tmp/output. Sehinnga command **ExecStart=/bin/sh -c “cat /root/root.txt > /tmp/output”** bertujuan agar file flag root.txt dapat dimunculkan di tmp/output.

**

**Answer : a58ff8579f0a9270368d33a9966c7fd5**