HACKTHEBOX

Informe Técnico

Máquina Horizontall

14 de abril del 2022

Índice

1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría realizada a la máquina **Horizontall** de la plataforma **HackTheBox**.

Figura 1: Dirección IP de la máquina

Dirección URL

Ir a la máquina.

2. Objetivos

Conocer el estado de seguridad actual del servidor **Horizontall**, enumerando posibles vectores de explotación y determinado alcance e impacto que un atacante podria ocasionar sobre el sistema en producción.

2.1. Consideraciones

Una vez finalizadas las joranadas de auditoría, se llevará a cabo una fase de saneamientos y buenas prácticas con el objetivo de securizar el servidor y evitar ser victimas de un futuro ataque en base a los vectores explotados.

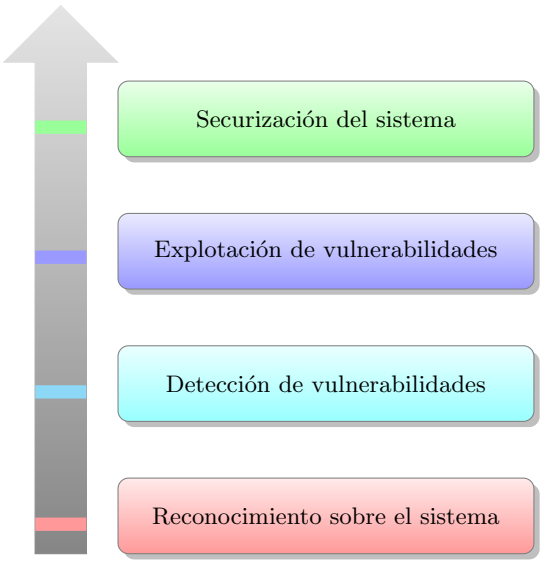

Figura 2: Flujo de trabajo

3. Analisis de vulnerabilidades

3.1. Vulnerabilidades encontradas

Se comenzó realizando un escaneo de puertos abiertos y escaneo de exhaustivo para poder ver como trabaja el sistema. Se observaron los puertos 22 y 80 abiertos, así que decidí investigar el puerto 80 para ver como era la pagina web. Despues de hacer la metodología de reconocimiento(FUZZ, CURL, etc...). Encontré una ruta interesante que tenia un archivo js por lo cual decidí investigar. Realizando un filtro en la petición de curl para ver si encontraba un subdominio, encontré uno el cual añadi en /etc/hosts para poder visualizar el contenido. Esta era una api. Por lo cual al ver que podia hacer volví a realizar un FUZZING pero ahora a la ruta encontrada y mostró una ruta interesante que ponía un panel de login en el CMS Strapi. Teniendo esta información procedí a realizar una busqueda de vulnerabilidades de este CMS y su versión, lo cual resutó exitoso ya que habian varios exploits. Tome uno que me permitira el RCE. Haciendo uso del exploit me puse en escucha para poder obtener una reverse shell, creando un archivo index.html con codigo en bash. Hice curl con un pipe en bash para que cuando descargara el archivo del servidor python que levanté se ejecutara y me diera la shell.

```
# Nmap 7.92 scan initiated Fri Apr  8 17:52:03 2022 as: nmap -sCV -p22,80 -oN targeted 10.10.11.105
Nmap scan report for 10.10.11.105
Host is up (0.077s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ee:77:41:43:d4:82:bd:3e:6e:6e:50:cd:ff:6b:0d:d5 (RSA)
|   256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
|_  256 4a:00:04:b4:9d:29:e7:af:37:16:1b:4f:80:2d:98:94 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-title: Did not follow redirect to http://horizontall.htb
|_http-server-header: nginx/1.14.0 (Ubuntu)
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 at Fri Apr  8 17:52:13 2022 -- 1 IP address (1 host up) scanned in 10.09 seconds
```

Figura 3: nmap

```
┌──(root㉿kali)-[/home/…/Machines/HTB/Horizontal/nmap]
└─# curl -s -X GET  "http://horizontall.htb/index.html"
<!DOCTYPE html><html lang=""><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial
-scale=1"><link rel="icon" href="/favicon.ico"><title>horizontall</title><link href="/css/app.0f40a091.css" rel="preload" as="style"><link href="/css/chunk-vendors.552
04a1e.css" rel="preload" as="style"><link href="/js/app.c68eb462.js" rel="preload" as="script"><link href="/js/chunk-vendors.0e02b89e.js" rel="preload" as="script"><li
nk href="/css/chunk-vendors.55204a1e.css" rel="stylesheet"><link href="/css/app.0f40a091.css" rel="stylesheet"></head><body><noscript><strong>We're sorry but horizonta
ll doesn't work properly without JavaScript enabled. Please enable it to continue.</strong></noscript><div id="app"></div><script src="/js/chunk-vendors.0e02b89e.js"><
/script><script src="/js/app.c68eb462.js"></script></body></html>
```

Figura 4: Curl a la pagina.

```
┌──(root㉿kali)-[/home/…/Machines/HTB/Horizontal/nmap]
└─# curl -s -X GET  "http://horizontall.htb/js/app.c68eb462.js" | grep "\.htb"
function(t){function s(s){for(var i,n,r=s[0],o=s[1],c=s[2],m=0,u=[];m<r.length;m++)n=r[m],Object.prototype.hasOwnProperty.call(a,n)&&a[n]&&u.push(a[n][0]),
 in o)Object.prototype.hasOwnProperty.call(o,i)&&(t[i]=o[i]);d&&d(s);while(u.length)u.shift()();return l.push.apply(l,c||[]),e()}function e(){for(var t,s=0
s++){for(var e=l[s],i=!0,r=1;r<e.length;r++){var o=e[r];0!==a[o]&&(i=!1)}i&&(l.splice(s--,1),t=n(n.s=e[0]))}return t}var i={},a={app:0},l=[];function n(s){
rn i[s].exports;var e=i[s]={i:s,l:!1,exports:{}};return t[s].call(e.exports,e,e.exports,n),e.l=!0,e.exports}n.m=t,n.c=i,n.d=function(t,s,e){n.o(t,s)||Objec
erty(t,s,{enumerable:!0,get:e})},n.r=function(t){"undefined"!==typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module
efineProperty(t,"__esModule",{value:!0})},n.t=function(t,s){if(1&s&&(t=n(t)),8&s)return t;if(4&s&&"object"===typeof t&&t&&t.__esModule)return t;var e=Objec
l);if(n.r(e),Object.defineProperty(e,"default",{enumerable:!0,value:t}),2&s&&"string"!=typeof t)for(var i in t)n.d(e,i,function(s){return t[s]}.bind(null,i
,n.n=function(t){var s=t&&t.__esModule?function(){return t["default"]}:function(){return t};return n.d(s,"a",s),s},n.o=function(t,s){return Object.prototyp
erty.call(t,s)},n.p="/";var r=window["webpackJsonp"]=window["webpackJsonp"]||[],o=r.push.bind(r);r.push=s,r=r.slice();for(var c=0;c<r.length;c++)s(r[c]);va
([0,"chunk-vendors"]),e()})({0:function(t,s,e){t.exports=e("56d7")},"034f":function(t,s,e){"use strict";e("85ec")},"1db9":function(t,s,e){t.exports=e.p+"im
1.jpg"},"215d":function(t,s){t.exports="
E1MOmNvbS5hZG9iZS54bXAAAAAAADw/eHBhY2tldCBiZWdpbj0i77u/IiBpZD0iVzVNME1wQ2VoaUh6cmVTek5UY3prYzlkIj8+IDx4OnhtcG1ldGEgeG1sbnM6eD0iYWRvYmU6bnM6bWV0YS8iIHg6eG1w
IFhNUCBDb3JlIDUuNi1jMDY3IDc5LjE1Nzc0NywgMjAxNS8wMy8zMC0yMzo0MDo0MiAgICAgICAgIj4gPHJkZjpSREYgeG1sbnM6cmRmPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5LzAyLzIyLXJkZi1zeW5
gPHJkZjpEZXNjcmlwdGlvbiByZGY6YWJvdXQ9IiIgeG1sbnM6eG1wPSJodHRwOi8vbnMuYWRvYmUuY29tL3hhcC8xLjAvIiB4bWxucDovL25zLmFkb2JlLmNvbS94YXAvMS4wL21tLy
RSZWY9Imh0dHA6Ly9ucy5hZG9iZS5jb20veGFwLzEuMC9zVHlwZS9SZXNvdXJjZVJlZiMiIHhtcDpDcmVhdG9yVG9vbD0iQWRvYmUgUGhvdG9zaG9wIENDIDIwMTUgKFdpbmRvd3MpIiB4bXBNTTpJbnN0Y
XAuaWlkOjJDNTQ4NTM3REI5MDExRTlCNDhGQTIwRjNGQTc1N0EzIiB4bXBNTTpEb2N1bWVudElEPSJ4bXAuZGlkOjJDNTQ4NTM4REI5MDExRTlCNDhGQTIwRjNGQTc1N0EzIj4gPHhtcE1NOkRlcml2ZWRG
Omluc3RhbmNlSUQ9InhtcC5paWQ6MkM1NDg1MzVEQjkwMTFFOUI0OEZBMjBGM0ZBNzU3QTMiIHN0UmVmOmRvY3VtZW50SUQ9InhtcC5kaWQ6MkM1NDg1MzZEQjkwMTFFOUI0OEZBMjBGM0ZBNzU3QTMiLz4
zY3JpcHRpb24+IDwvcmRmOlJERj4gPC94OnhtcG1ldGE+IDw/eHBhY2tldCBlbmQ9InIiPz4FAS0XAAAJWElEQVR42uxdaYwURRSuGWYvDtldBBY8gAVFMCBI5PDCA6IiHtFoVBTjgmi8DRiDIREP0OBF1I
DxwAO5vBYURCECQRQ5FtiDZW/fl34d23Gmu6q7Z3p6p77kCxumurq6672qVV69evY6UlpYKl8glDiEOJQ4m9iDmEzsQ84jNxAbiMWYlcQdxL3E7cRNxC7FFaGgEjJiLa64k3kYcTWzn8f4VxDXEN4jvtqL3W
By2KSOD9sS2NnVEiY3EQyGRxUL+O9ng2IYH1GN+3zyiMCPcTnyK2ClFLwKddR3xM5X2syAc8yhQfuM7ni1rbQQUs+aDxNku71HIM2o3m/vksvBcTlyR4YrwDHEK92WLzQCzjHiF3zePSpQ5jbiTOC+FSgAU
```

Figura 5: Filtrando contenido del archivo js.

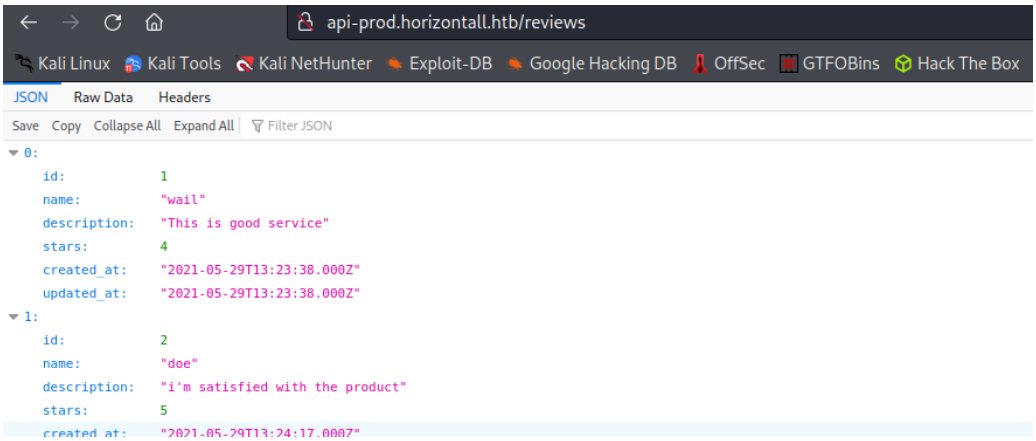

Figura 6: Viendo la subdominio encontrado.

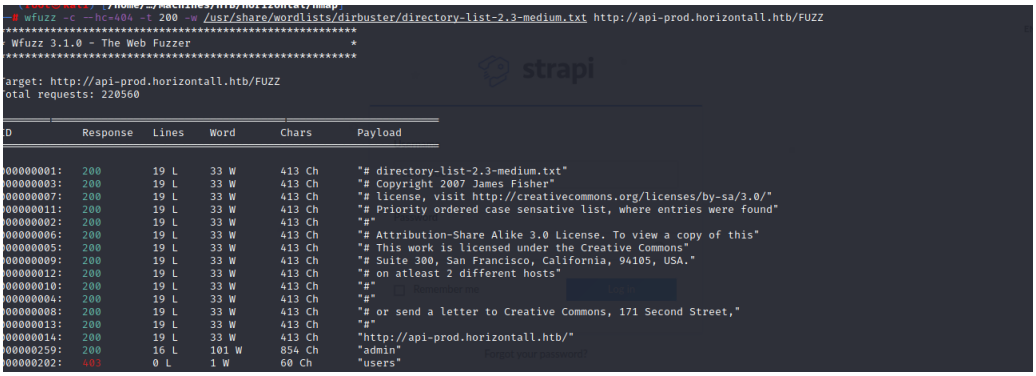

Figura 7: Aplicando FUZZING a la ruta.

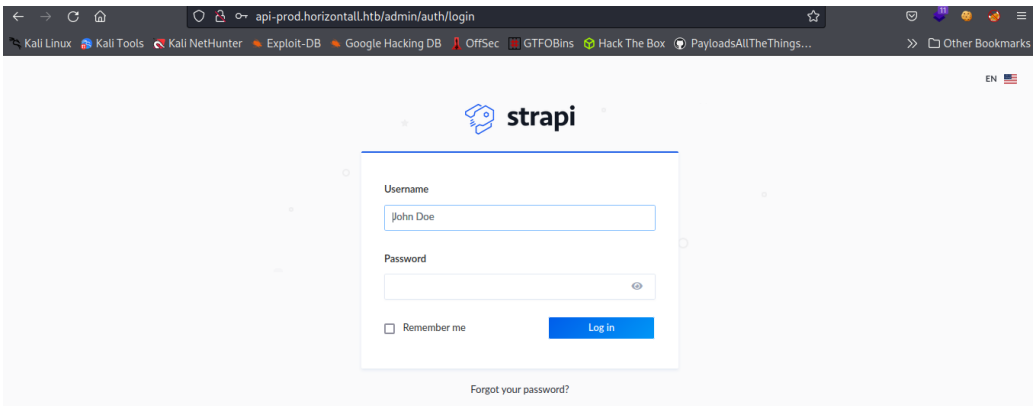

Figura 8: Login del CMS Strapi.

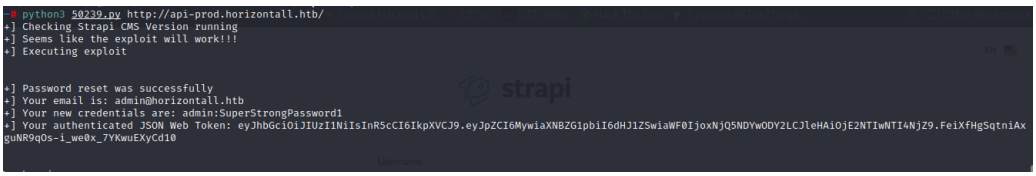

Figura 9: Haciendo uso del exploit para Strapi.

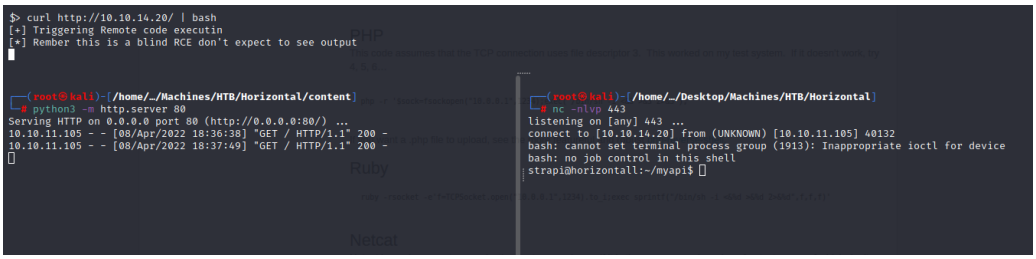

Figura 10: Obteniendo reverse shell usuario.

Se procedió a escalar los privilegios, haciendo la metodología correspondiente de posibles vias de escalar al listar los puertos de la maquina me encontré con uno bastante curioso el 8000. Así que procedí a utilizar la herramienta chisel para hacer Remote Port Forwarding y que el puerto 8000 de la maquina lo interpretara como mi puerto en el localhost. Esto mostraba una pagina en lavarel, procedí a buscar exploits y vulnerabilidades de la versión que se estaba ejecutando, de igual manera encontré uno, hice el mismo paso para obtener la reverse shell de usuario, pero con este exploit y listo.

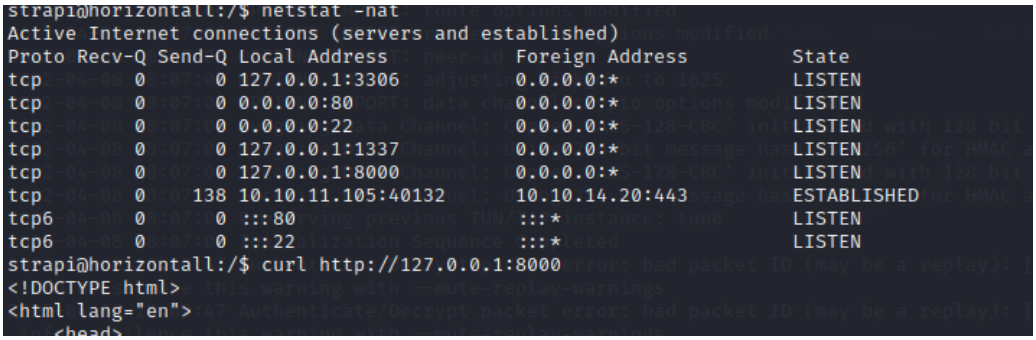

Figura 11: Listando puertos de la maquina.

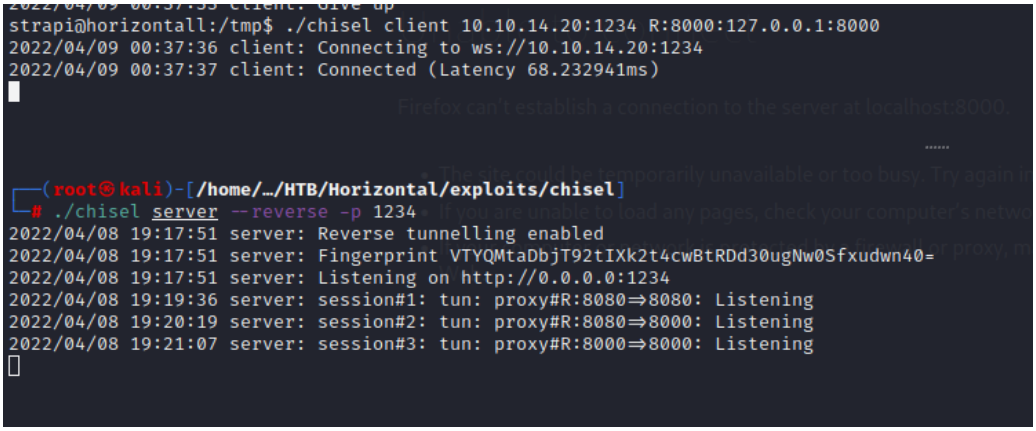

Figura 12: Aplicando remote port forwarding

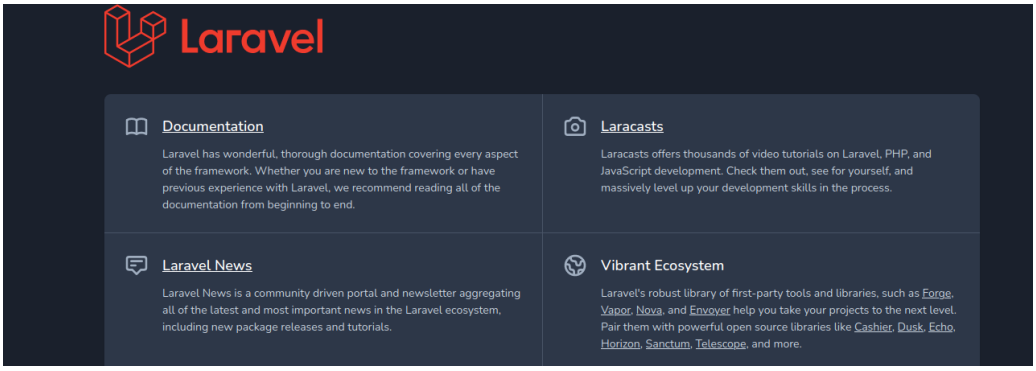

Figura 13: Contenido del puerto 8000

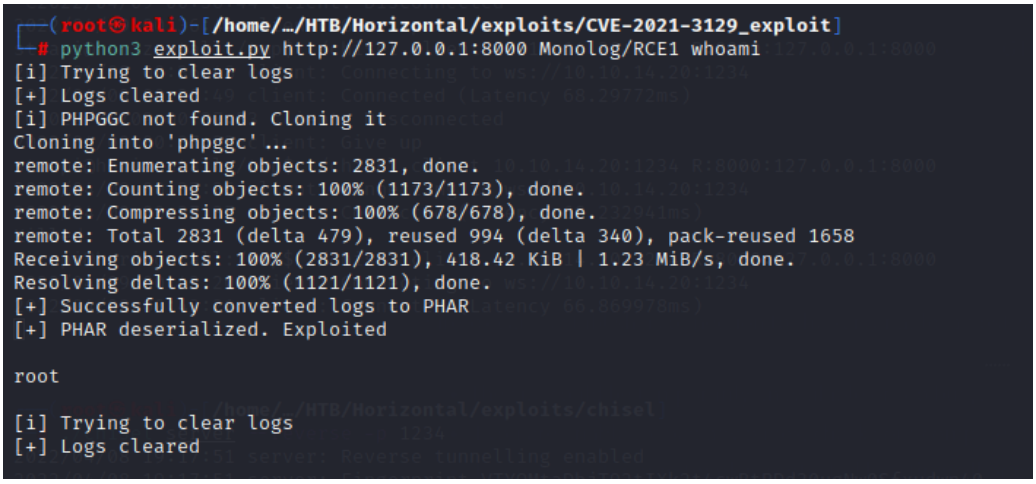

Figura 14: Probando el exploit de lavarel.

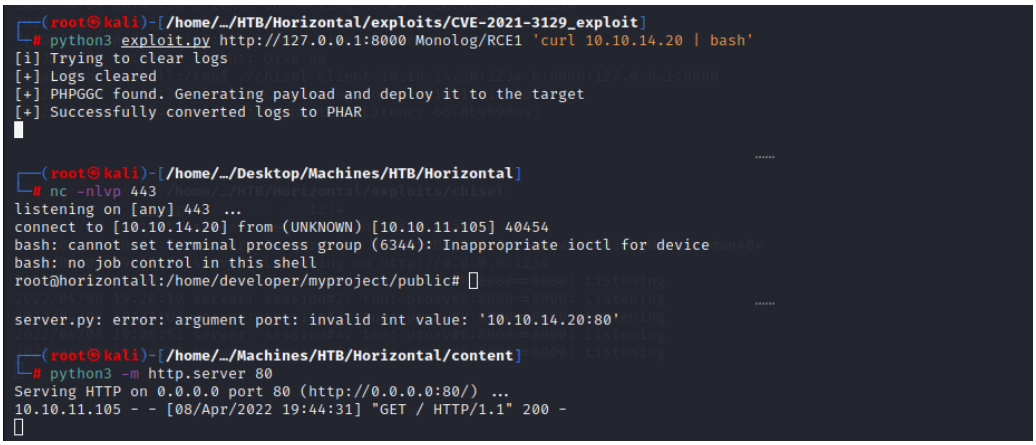

Figura 15: Maquina pwneada.