



## HTB Writeups by m15t

Name: Titanic

Type: Machine

OS: Linux

Difficulty: Easy

Points: 30

### Important:

This is still an active machine, this writeup should not be shared outside this platform because it violates HTB terms and conditions and may result to a possible ban or punishment.

### Description:

This is a writeup to get user.txt on the box. For root.txt stay tuned!! Let us begin

First begin with connecting to the HTB vpn like below:

```
m15t@neblina: ~/Downloads
(m15t@neblina)~[~]
$ dwns

(m15t@neblina)~[~/Downloads]
$ 0vpn lab_m15t.ovpn
[sudo] password for m15t:
2025-02-19 13:15:58 WARNING: Compression for receiving enabled. Compression has
been used in the past to break encryption. Sent packets are not compressed unles
s "allow-compression yes" is also set.
2025-02-19 13:15:58 Note: --data-ciphers-fallback with cipher 'AES-128-CBC' disa
bles data channel offload.
2025-02-19 13:15:58 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ
4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-19 13:15:58 library versions: OpenSSL 3.4.0 22 Oct 2024, LZO 2.10
2025-02-19 13:15:58 DCO version: N/A
2025-02-19 13:15:58 TCP/UDP: Preserving recently used remote address: [AF_INET]1
54.57.165.190:1337
2025-02-19 13:15:58 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-02-19 13:15:58 UDPv4 link local: (not bound)
2025-02-19 13:15:58 UDPv4 link remote: [AF_INET]154.57.165.190:1337
2025-02-19 13:15:58 TLS: Initial packet from [AF_INET]154.57.165.190:1337, sid=5
5b58d45 c104acdd
2025-02-19 13:15:59 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB
VPN: Root Certificate Authority
```

**Note:** These are not the commands to do the tasks these are my custom commands.

dwns= cd Downloads & 0vpn= sudo openvpn --config



Now use this command to know the domain name for the machine via the ip given like below:

```
m15t@neblina: ~  
  
(m15t@neblina)-[~]  
$ curl -X POST 10.10.11.55 -i  
HTTP/1.1 301 Moved Permanently  
Date: Wed, 19 Feb 2025 19:22:57 GMT  
Server: Apache/2.4.52 (Ubuntu)  
Location: http://titanic.htb/  
Content-Length: 304  
Content-Type: text/html; charset=iso-8859-1  
  
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>301 Moved Permanently</title>  
</head><body>  
<h1>Moved Permanently</h1>  
<p>The document has moved <a href="http://titanic.htb/">here</a>.</p>  
<hr>  
<address>Apache/2.4.52 (Ubuntu) Server at 10.10.11.55 Port 80</address>  
</body></html>  
  
(m15t@neblina)-[~]  
$ sudo echo "10.10.11.55 titanic.htb" | sudo tee /etc/hosts  
10.10.11.55 titanic.htb
```

Next step is to do our nmap scan to know what ports are open on the machine. Use this command for OS info, Service version etc: We see two ports open (80 “http” and 22 “ssh”)

```
m15t@neblina: ~  
  
(m15t@neblina)-[~]  
$ nmap -sCV -A titanic.htb  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 13:24 CST  
Nmap scan report for titanic.htb (10.10.11.55)  
Host is up (0.29s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   256 73:03:9c:76:eb:04:f1:fe:c9:e9:80:44:9c:7f:13:46 (ECDSA)  
|_  256 d5:bd:1d:5e:9a:86:1c:eb:88:63:4d:5f:88:4b:7e:04 (ED25519)  
80/tcp    open  http      Apache httpd 2.4.52  
|_ http-server-header: Apache/2.4.52 (Ubuntu)
```

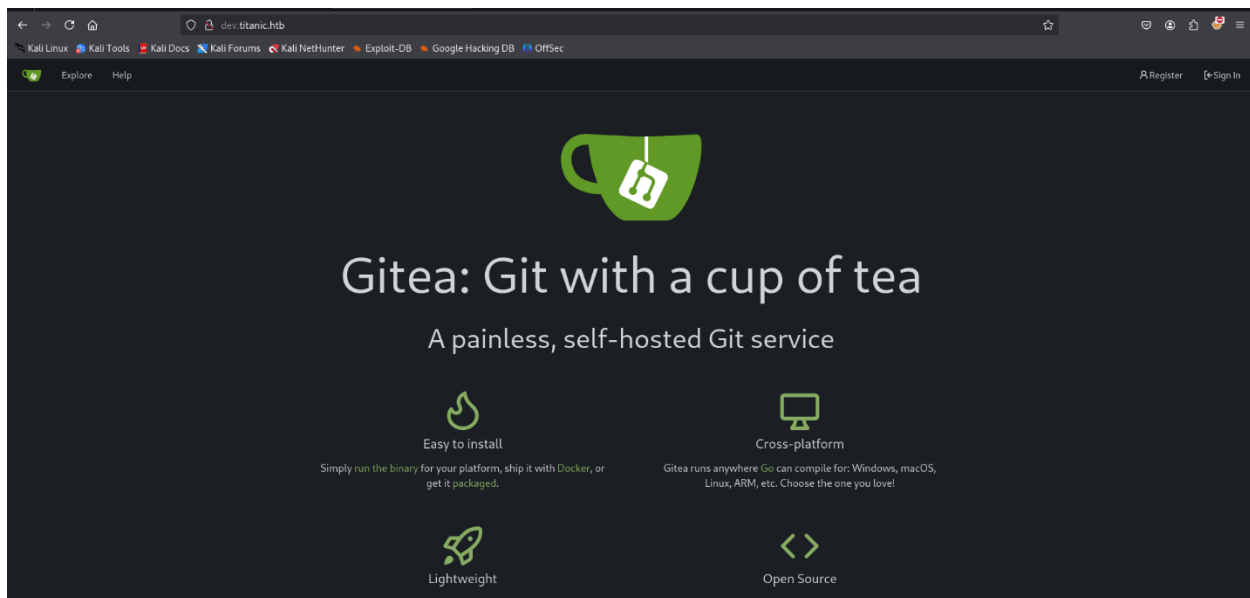


So before I check the page on port 80, I run ffuf to try and find some subdomains on the box and it seems we only got one hit with the command below:

```
m15t@neblina: ~  
m15t@neblina:~$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -H "Host:FUZZ.titanic.htb" -u http://titanic.htb -fs 169 | grep 'Status: 200'  
  
v2.1.0-dev  
-----  
:: Method      : GET  
:: URL         : http://titanic.htb  
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt  
:: Header      : Host: FUZZ.titanic.htb  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads    : 40  
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500  
:: Filter      : Response size: 169  
-----  
dev [Status: 200, Size: 13982, Words: 1107, Lines: 276, Duration: 239ms]  
:: Progress: [958/43007] :: Job [1/1] :: 88 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

**Note:** You can use what you're comfortable with. I use ffuf a lot but even gobster can do the trick too.

Now add dev.titanic.htb to /etc/hosts so you can access it via web. Now lets got titanic.htb and also dev.titanic.htb to see what we have running on there. We see that gitea is on dev.titanic.htb. We will get back to that later. Got to titanic.htb.





Now on titanic.htb we see this static page. Click around and see that nothing is happening but when we click the “Book Now” we see some form pop up. Lets fill in and see what happens upon submit:

Book Your Trip

Full Name  
m15t

Email address  
m15t@titanic.htb

Phone Number  
123456789

Travel Date  
02 / 12 / 2000

Cabin Type  
Deluxe

Submit

Upon clicking submit we see that a file is downloaded. We open the file and we see that it just shows the info we entered. Not too useful but then again this might mean there should be a download directory? Lets try adding a /download to the url and see what happens cause I did a dirb scan and only hit /book so this is me trusting my hunches.

Book Your Trip

Full Name  
m15t

Email address  
m15t@titanic.htb

Phone Number  
123456789

Travel Date  
02 / 12 / 2000

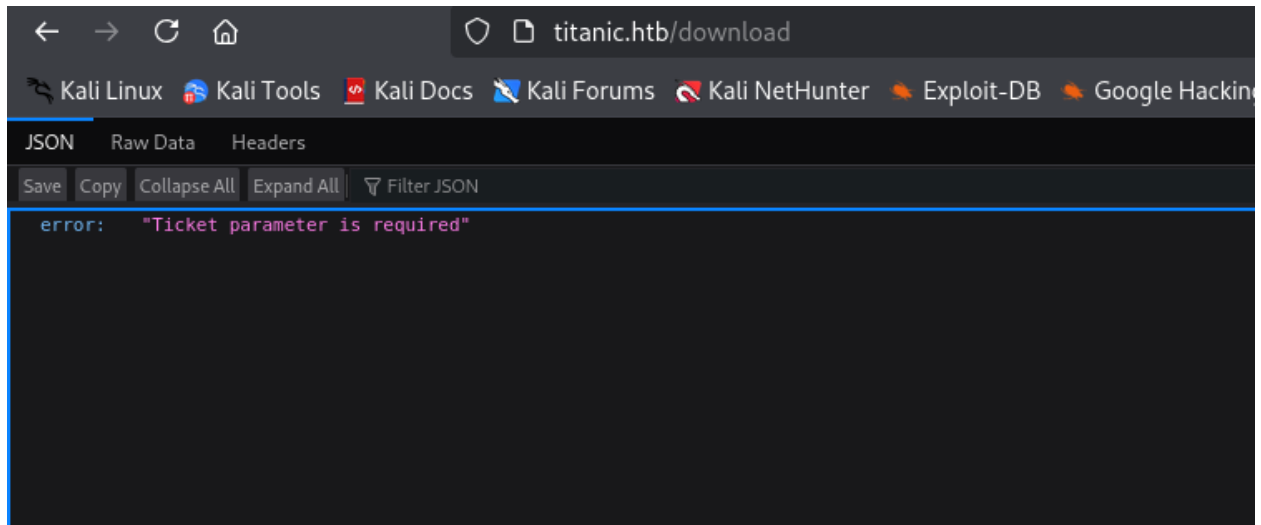
Cabin Type  
Deluxe

Submit

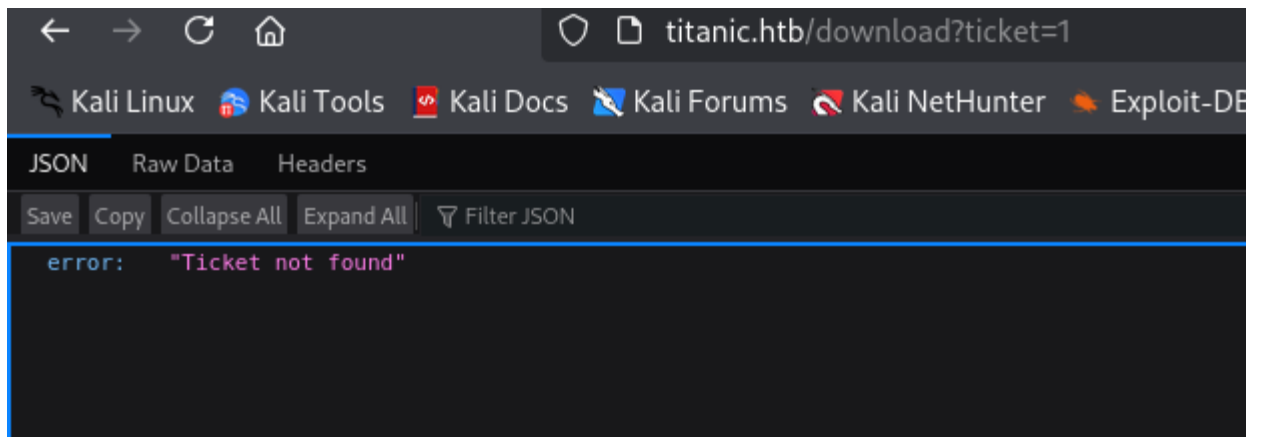
Download notification:  
fde2a30a-c3c6-41a2-966f-53488b5469c2.json Completed — 108 bytes  
09ed2e3d-0722-467c-9faa-2ba04d07c6cb.json Completed — 109 bytes  
Show all downloads



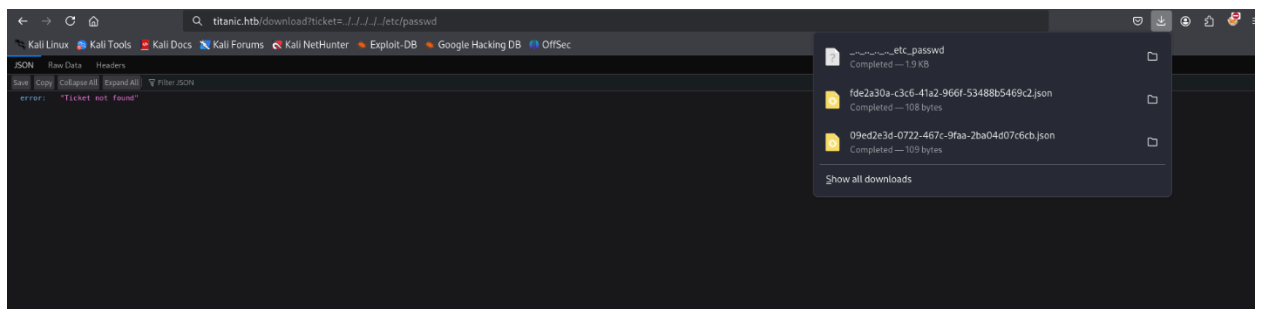
Upon hitting /download we see this message “Ticket parameter is required”



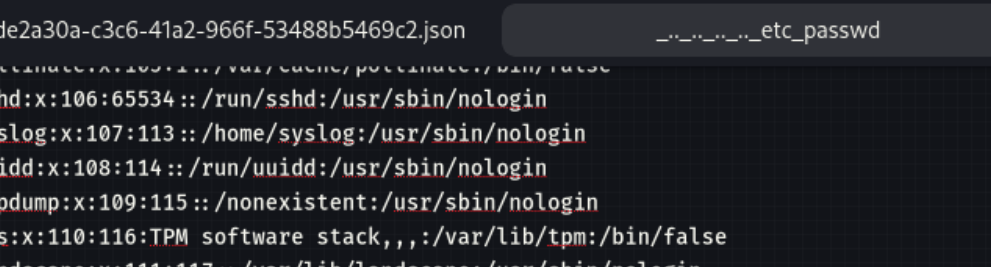
Upon seeing this I asked ChatGPT what this message meant and it told me that the page might be collecting tickets and that I should try ticket=id so I tried like below:



We see that it responds with “Ticket not found” so I tried an lfi attempt via the url to see if it is vulnerable to lfi:



It downloads the file `/etc/passwd`. Upon checking it I realise that it is vulnerable to LFI LMAO:

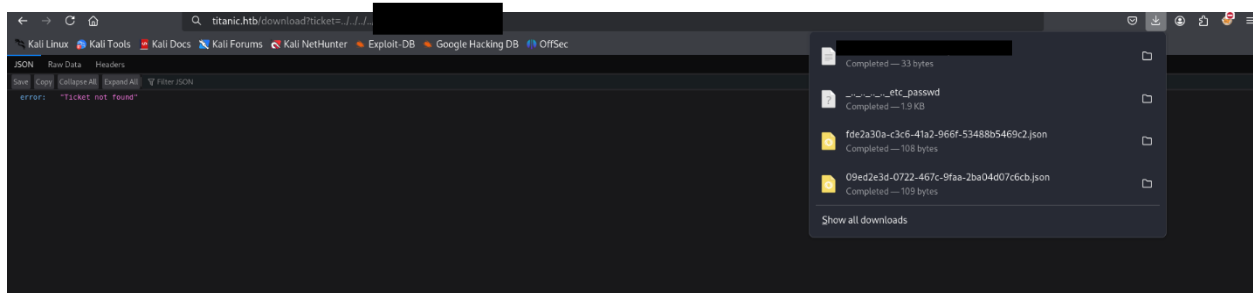


```
Open  ~/.Downloads/..._etc_passwd
fde2a30a-c3c6-41a2-966f-53488b5469c2.json  ..._etc_passwd x
pottannc:x:105:1::/var/cache/pottannc:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uidd:x:108:114::/run/uidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin

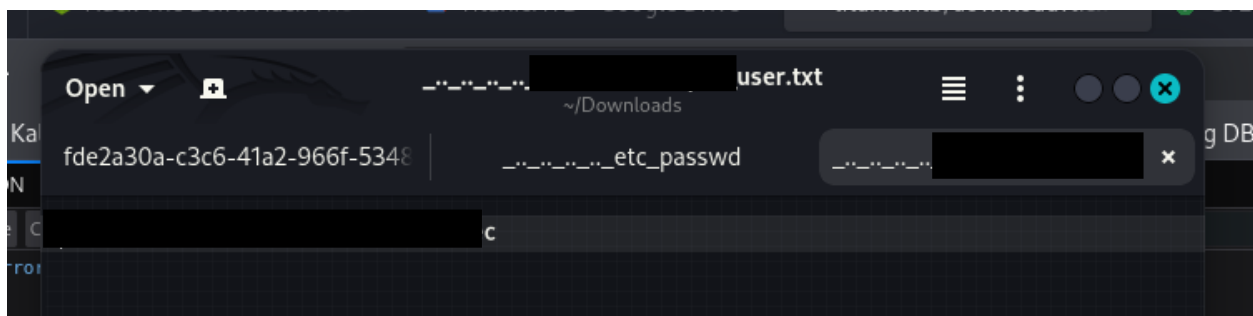
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false
```

**Important:**

Go through the `/etc/passwd` file there's something that is very useful for the next part. Considering we found the useful string important for the next part, lets get `user.txt` using `lfi`.



We open the downloaded user.txt file and boom we have user.txt.







### Conclusion:

Method to get root.txt on the titanic machine will be released when the machine retires. But that doesn't mean you stop trying to get root. That was all and this is the simplest way to get user.txt cause there's another method which I initially used involving burp suite and getting a reverse shell on the box then getting user.txt and then escalating privileges. Happy Hacking y'all my name is m15t.

Please give me feedback on how my writeup was considering this is when I am actually beginning to create writeups of machines I complete.

**Remember: This writeup is not to be shared with the public before the machine retires!!!**

