TryHackMe – Vulnversity

Contents

[Nmap 2](#_Toc147764802)

[Gobuster 2](#_Toc147764803)

[Escalation 3](#_Toc147764804)

[Upgrade Shell 3](#_Toc147764805)

[Flag 1 3](#_Toc147764806)

[Finding Binaries 3](#_Toc147764807)

[Exploiting Systemctl 3](#_Toc147764808)

[Flag 2 4](#_Toc147764809)

# Nmap



A computer screen with white text

Description automatically generated







# Gobuster

A blue square with white text

Description automatically generatedI renamed the file to shell2.phtml, since regular php files are not accepted.

A close-up of words

Description automatically generated

A black background with white text

Description automatically generated

# Escalation

## Upgrade Shell



A screen shot of a computer code

Description automatically generated



# Flag 1

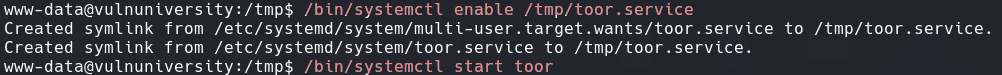
# Finding Binaries





# A computer screen shot of a black screen Description automatically generatedExploiting Systemctl

**Article used**: https://medium.com/@klockw3rk/privilege-escalation-leveraging-misconfigured-systemctl-permissions-bc62b0b28d49

After creating toor.service, I then ran the commands below (must have SUID bit set).

A computer screen with white text

Description automatically generatedBefore running the last command I set up a netcat listener in the terminal.

# Flag 2

A black background with white text

Description automatically generated

The root flag was located in /root.