

TryHackMe — Jr Penetration Tester | Introduction to Web Hacking |Part-1



Aditya Sharma · Follow

4 min read · Oct 20, 2021




Listen



Share



... More

This would be the second write-up for our series of TryHackMe learning Path- **Jr Penetration Tester**. This chapter contains 10 rooms, this will be the first part having write-ups for first 5 rooms.





Introduction to Web Hacking



Get hands-on, learn about and exploit some of the most popular web application vulnerabilities seen in the industry today.

-  



Walking An Application

Manually review a web application for security issues using only your browsers developer tools. Hacking with just your browser, no tools or scripts.
-  



Content Discovery

Learn the various ways of discovering hidden or private content on a webserver that could lead to new vulnerabilities.
-  

Subdomain Enumeration

Learn the various ways of discovering subdomains to expand your attack surface of a target.
-  

Authentication Bypass

Learn how to defeat logins and other authentication mechanisms to allow you access to unpermitted areas.
-  

IDOR

Learn how to find and exploit IDOR vulnerabilities in a web application giving you access to data that you shouldn't have.

*Our second Chapter in this path would be, **Introduction to Web Hacking**- Get hands-on, learn about and exploit some of the most popular web application vulnerabilities seen in the industry today.*

*Our first room would be, **Walking An Application**- Manually review a web application for security issues using only your browsers developer tools. Hacking with just your browser, no tools or scripts.*

Task-1 Walking An Application

Q. Read Only

Task-2 Exploring The Website

Q. Read Only

Task-3 Viewing The Page Source

Q. What is the flag from the HTML comment?

A. THM{HTML_COMMENTS_ARE_DANGEROUS}

Q. What is the flag from the secret link?

A. THM{NOT_A_SECRET_ANYMORE}

Q. What is the directory listing flag?

A. THM{INVALID_DIRECTORY_PERMISSIONS}

Q. What is the framework flag?

A. THM{KEEP_YOUR_SOFTWARE_UPDATED}

Task-4 Developer Tools — Inspector

Q. What is the flag behind the paywall?

A. THM{NOT_SO_HIDDEN}

Task-5 Developer Tools — Debugger

Q. What is the flag in the red box?

A. THM{CATCH_ME_IF_YOU_CAN}

Task-6 Developer Tools — Network

Q. What is the flag shown on the contact-msg network request?

A. THM{GOT_AJAX_FLAG}

*Our second room would be **Content Discovery**- Learn the various ways of discovering hidden or private content on a webserver that could lead to new vulnerabilities.*

Task-1 What Is Content Discovery?

Q. What is the Content Discovery method that begins with M?

A. Manually

Q. What is the Content Discovery method that begins with A?

A. Automated

Q. What is the Content Discovery method that begins with O?

A. OSINT

Task-2 Manual Discovery — Robots.txt

Q. What is the directory in the robots.txt that isn't allowed to be viewed by web crawlers?

A. /staff-portal

Task-3 Manual Discovery — Favicon

Q. What framework did the favicon belong to?

A. cgiirc (MD5- f276b19aabc4ae8cda4d22625c6735f)

Task-4 Manual Discovery — Sitemap.xml

Q. What is the path of the secret area that can be found in the sitemap.xml file?

A. /s3cr3t-area

Task-5 Manual Discovery — HTTP Headers

Q. What is the flag value from the X-FLAG header?

A. THM{HEADER_FLAG}

Task-6 Manual Discovery — Framework Stack

Q. What is the flag from the framework's administration portal?

A. THM{CHANGE_DEFAULT_CREDENTIALS}

Task-7 OSINT — Google Hacking / Dorking

Q. What Google dork operator can be used to only show results from a particular site?

A. site:

Task-8 OSINT — Wappalyzer

Q. What online tool can be used to identify what technologies a website is running?

A. Wappalyzer

Task-9 OSINT — Wayback Machine

Q. What is the website address for the Wayback Machine?

A. <https://archive.org/web/>

Task-10 OSINT — GitHub

Open in app ↗



Search



Task-11 OSINT — S3 Buckets

Q. What URL format do Amazon S3 buckets end in?

A- .s3.amazonaws.com

Task-12 Automated Discovery

Q. What is the name of the directory beginning “/mo....” that was discovered?

A. /monthly

Q. What is the name of the log file that was discovered?

A. /development.log

*Our third room would be- **Subdomain Enumeration**, Learn the various ways of discovering subdomains to expand your attack surface of a target.*

Task-1 Brief

Q. What is a subdomain enumeration method beginning with B?

A. Brute Force

Q. What is a subdomain enumeration method beginning with O?

A. OSINT

Q. What is a subdomain enumeration method beginning with V?

A. Virtual Host

Task-2 OSINT — SSL/TLS Certificates

Q. What domain was logged on crt.sh at 2020-12-26?

A. store.tryhackme.com

Task-3 OSINT — Search Engines

Q. What is the TryHackMe subdomain beginning with B discovered using the above Google search?

A. blog.tryhackme.com

Task-4 DNS Bruteforce

Q. What is the first subdomain found with the dnsrecon tool?

A. api.acmeitsupport.thm

Task-5 OSINT — Sublist3r

Q. What is the first subdomain discovered by sublist3r?

A. web55.acmeitsupport.thm

Task-6 Virtual Hosts

Q. What is the first subdomain discovered?

A. delta

Q. What is the second subdomain discovered?

A. yellow

*Our fourth room is **Authentication Bypass**- Learn how to defeat logins and other authentication mechanisms to allow you access to unpermitted areas.*

Task-1 Brief

Q. Read Only

Task-2 Username Enumeration

Q. What is the username starting with si*** ?

A. simon

Q. What is the username starting with st*** ?

A. steve

Q. What is the username starting with ro**** ?

A. robert

Task-3 Brute Force

Q. What is the valid username and password (format: username/password)?

A. steve/thunder

Task-4 Logic Flaw

Q. What is the flag from Robert's support ticket?

A. THM{AUTH_BYPASS_COMPLETE}

Task-5 Cookie Tampering

Q. What is the flag from changing the plain text cookie values?

A. THM{COOKIE_TAMPERING}

Q. What is the value of the md5 hash 3b2a1053e3270077456a79192070aa78 ?

A. 463729

Q. What is the base64 decoded value of VEhNe0JBU0U2NF9FTkNPRElOR30= ?

A. THM{BASE64_ENCODING}

Q. Encode the following value using base64 {"id":1,"admin":true}

A. eyJpZCI6MSwiYWRTaW4iOnRydWV9

*Our fifth room would be **IDOR**- Learn how to find and exploit IDOR vulnerabilities in a web application giving you access to data that you shouldn't have.*

Task-1 What is an IDOR?

Q. What does IDOR stand for?

A. Insecure Direct Object Reference

Task-2 An IDOR Example

Q. What is the Flag from the IDOR example website?

A. THM{IDOR-VULN-FOUND}

Task-3 Finding IDORs in Encoded IDs

Q. What is a common type of encoding used by websites?

A. base64

Task-4 Finding IDORs in Hashed IDs

Q. What is a common algorithm used for hashing IDs?

A. MD5

Task-5 Finding IDORs in Unpredictable IDs

Q. What is the minimum number of accounts you need to create to check for IDORs between accounts?

A. 2

Task-6 Where are IDORs located

Q. Read Only

Task-7 A Practical IDOR Example

Q. What is the username for user id 1?

A. adam84

Q. What is the email address for user id 3?

A. j@fakemail.thm

Web Hacking

Tryhackme

Tryhackme Walkthrough

Pentesting



Follow



Written by Aditya Sharma

347 Followers

In an effort to protect the globe!

More from Aditya Sharma

Task 1	✓	Introduction	▼
Task 2	✓	What is Privilege Escalation?	▼
Task 3	✓	Enumeration	☰ ▼
Task 4	✓	Automated Enumeration Tools	▼
Task 5	✓	Privilege Escalation: Kernel Exploits	☰ ▼
Task 6	✓	Privilege Escalation: Sudo	☰ ▼
Task 7	✓	Privilege Escalation: SUID	☰ ▼
Task 8	✓	Privilege Escalation: Capabilities	☰ ▼
Task 9	✓	Privilege Escalation: Cron Jobs	☰ ▼
Task 10	✓	Privilege Escalation: NFS	☰ ▼

 Aditya Sharma

TryHackMe— Jr Penetration Tester | Privilege Escalation | Linux Privesc | Part 2

This would be the much awaited, the fourteenth and the last write-up for our series of TryHackMe learning Path- Jr Penetration Tester.

5 min read · Oct 27, 2021



73



3



100%	
Task 1	Brief
Task 2	What is a Database?
Task 3	What is SQL?
Task 4	What is SQL Injection?
Task 5	In-Band SQLi
Task 6	Blind SQLi - Authentication Bypass
Task 7	Blind SQLi - Boolean Based
Task 8	Blind SQLi - Time Based
Task 9	Out-of-Band SQLi

 Aditya Sharma

TryHackMe— Jr Penetration Tester | Introduction to Web Hacking | SQL Injection | Part-5

This would be the eighth write-up for our series of TryHackMe learning Path- Jr Penetration Tester. This chapter contains 10 rooms,

3 min read · Oct 24, 2021



26



1



Introduction to Pentesting

stand what a penetration test involves, including testing techniques and methodology that a pentester should know.



Pentesting Fundamentals

Learn the important ethics and methodologies behind every pentest



Principles of Security

Learn the principles of information security that secures data and protects systems from a

 Aditya Sharma

TryHackMe—Jr Penetration Tester (Introduction to Pentesting)

This would be the a new series in the write-up for the TryHackMe, We will start with the learning path- Jr Penetration Tester.

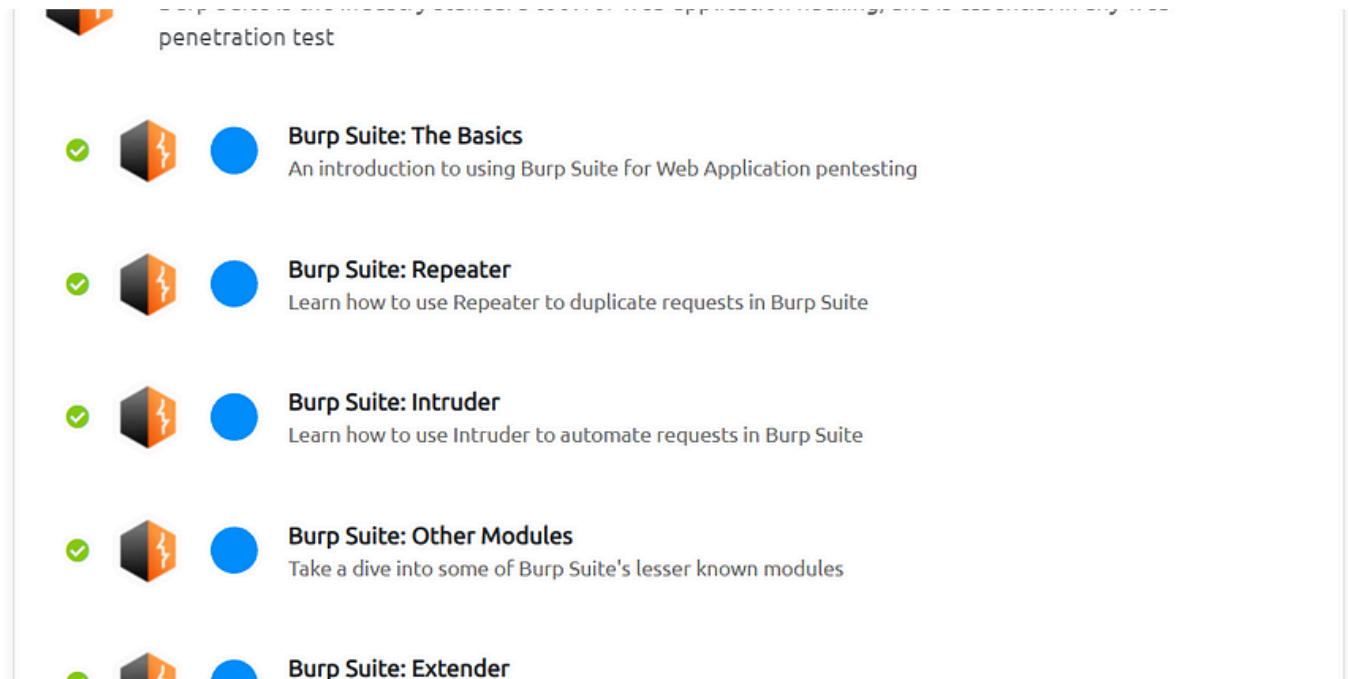
3 min read · Oct 19, 2021



6



2



Aditya Sharma

TryHackMe—Jr Penetration Tester | Burp Suite

This would be the seventh write-up in the learning path Jr Penetration Tester series. We will start with the chapter Burp Suite- It is the...

6 min read · Oct 23, 2021



73

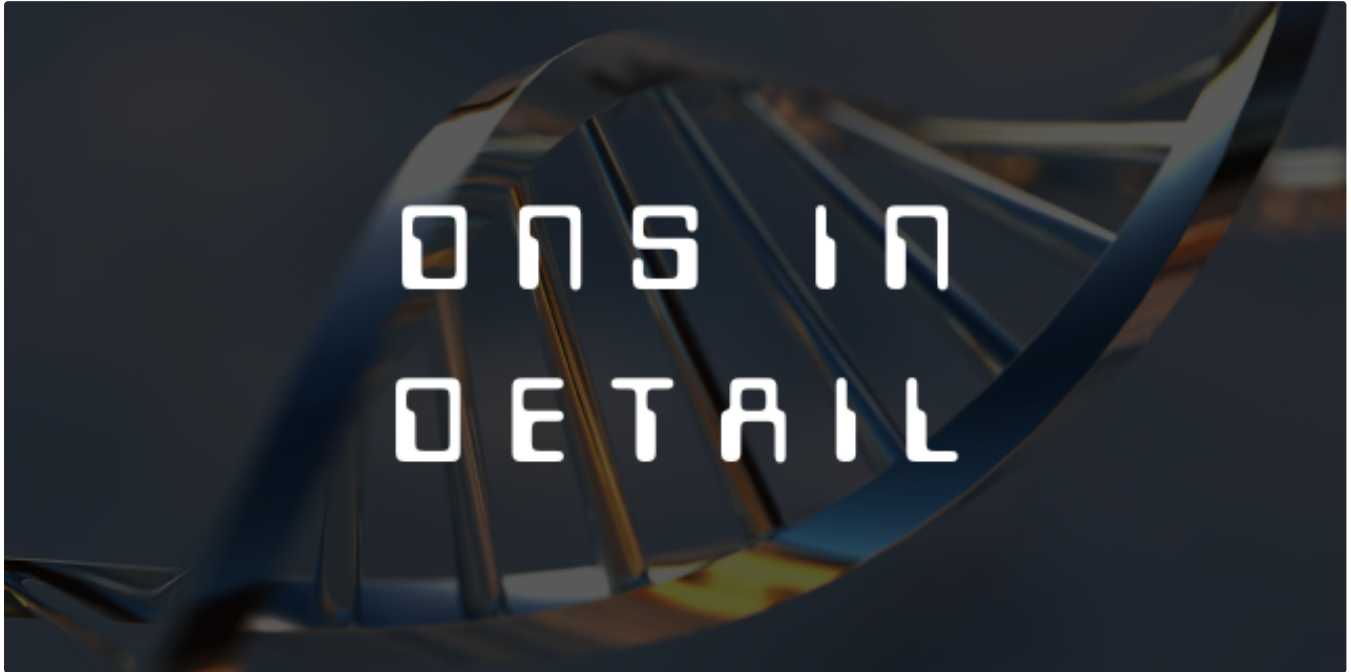



5



See all from Aditya Sharma

Recommended from Medium



 Hammaad M

TryHackMe, DNS In Detail

Learn how DNS works and how it helps you access internet services...

5 min read · Dec 7, 2023



```
PS C:\Users\thm-unpriv> ls

Directory: C:\Users\thm-unpriv

Mode                LastWriteTime         Length Name
----                -
d-r--             5/3/2022   3:14 PM             3D Objects
d-r--             5/3/2022   3:14 PM             Contacts
d-r--             5/4/2022   8:15 AM             Desktop
d-r--             5/3/2022   3:14 PM             Documents
d-r--             5/3/2022   3:14 PM             Downloads
d-r--             5/3/2022   3:14 PM             Favorites
d-r--             5/3/2022   3:14 PM             Links
d-r--             5/3/2022   3:14 PM             Music
d-r--             5/3/2022   3:14 PM             Pictures
d-r--             5/3/2022   3:14 PM             Saved Games
d-r--             5/3/2022   3:14 PM             Searches
d-r--             5/3/2022   3:14 PM             Videos
-a---            11/10/2023  11:52 AM          48640 rev-svc.exe
```



James Jarvis

Windows Privilege Escalation | TryHackMe

Another day, another room. Today I am undertaking the Windows Privilege Escalation room.

14 min read · Nov 10, 2023



21

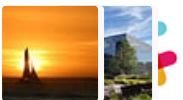


Lists



Staff Picks

629 stories · 918 saves



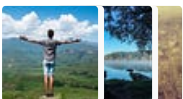
Stories to Help You Level-Up at Work

19 stories · 575 saves



Self-Improvement 101

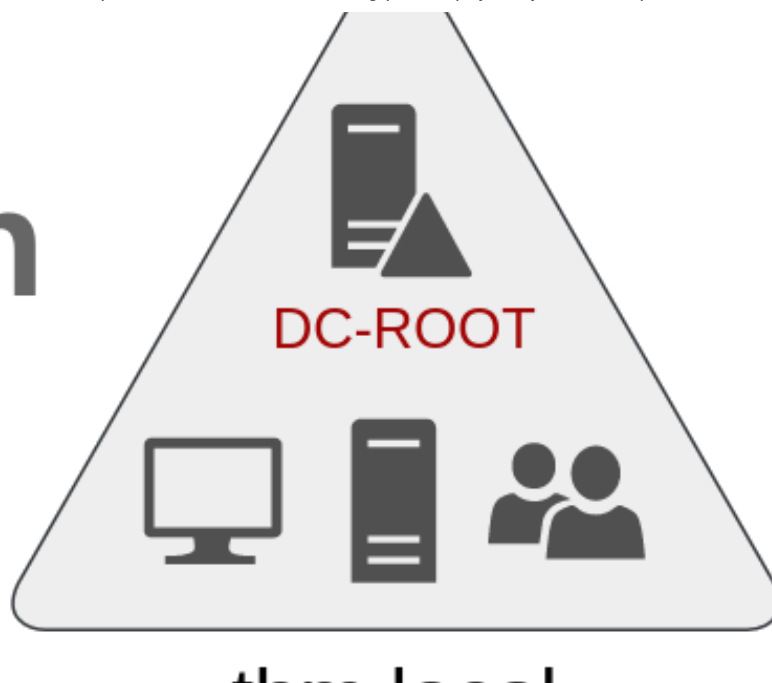
20 stories · 1665 saves




Productivity 101

20 stories · 1534 saves

Domain



 Rahul Kumar

Active Directory Basics | Tryhackme Walkthrough

This room will introduce the basic concepts and functionality provided by Active Directory.

25 min read · Mar 20, 2024



5



positions

payloads

resource pool

settings

?

Choose an attack type

Start attack

Attack type:

Sniper

?

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:

https://10-10-98-200.p.thmlabs.com

☒ Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

1

POST /support/login/ HTTP/1.1

2

Host: 10-10-98-200.p.thmlabs.com

3

Content-Length: 37

4

Cache-Control: max-age=0

5

Sec-Ch-Ua:

6

Sec-Ch-Ua-Mobile: ?0

7

Sec-Ch-Ua-Platform: ""

8

Upgrade-Insecure-Requests: 1

9

Origin: https://10-10-98-200.p.thmlabs.com

10

Content-Type: application/x-www-form-urlencoded

11

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.159 Safari/537.36

12

Accept:

13

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

14

Sec-Fetch-Site: same-origin

15

Sec-Fetch-Mode: navigate

16

Sec-Fetch-User: ?1

17

Sec-Fetch-Dest: document

18

Referer: https://10-10-98-200.p.thmlabs.com/support/login/

19

Accept-Encoding: gzip, deflate

20

Accept-Language: en-US,en;q=0.9

21

Connection: close

22

username=\$pentester\$password=\$Exp10lt3d\$

 Ayan Mukherjee

TryHackMe: Burp Suite: Intruder

Intruder is an important part of Burp Suite. But in general, except just to do a simple recursive requests, Intruder can be made much...

8 min read · Nov 6, 2023



21



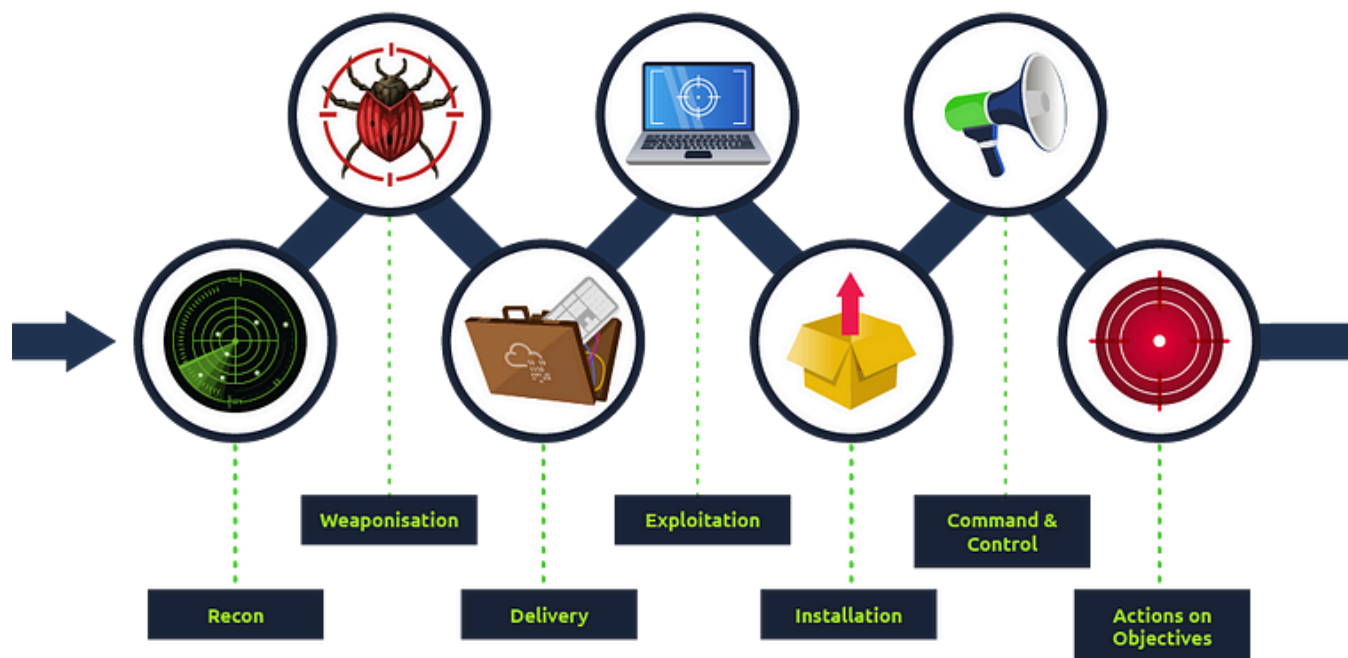
CyberNet

TryHackMe—Kenobi CTF Writeup/Walkthrough

The Kenobi room on TryHackMe is focused This room will cover accessing a Samba share, manipulating a vulnerable version of proftpd to gain...

7 min read · Jan 19, 2024





L L4V4NY4 AGR3

Network Security

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

10 min read · Dec 11, 2023



12



See more recommendations