

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



Data Exfiltration-THM



0xUN7H1NK4BLE · [Follow](#)

2 min read · Dec 13, 2022



Listen



Share

... More

In which case scenario will sending and receiving traffic continue during the connection?

Tunneling

In which case scenario will sending and receiving traffic be in one direction?

traditional data exfiltration

In the next task, we will be discussing how data exfiltration over the TCP socket works!

--

Exfiltration using TCP sockets relies on _____ protocols!

non-standard

Now apply what we discussed to exfiltrate data over the TCP socket! Once you exfiltrate data successfully, hit **Completed** to move on to the next task!

—

All packets sent using the Data Exfiltration technique over SSH are encrypted!
(T=True/F=False)

T

Replicate the steps to transfer data over the SSH client. Once you transfer the file successfully, hit **Completed** and move on to the next task!

—

Check the Apache log file on web.thm.com and get the flag!

THM{H77P-G37-15-f0un6}

When you visit the <http://flag.thm.com/flag> website through the uploader machine via the HTTP tunneling technique, what is the flag?

THM{H77p_7unn3l1n9_l1k3_l337}

In which ICMP packet section can we include our data?

Data

Follow the technique discussed in this task to establish a C2 ICMP connection between JumpBox and ICMP-Host. Then execute the “getFlag” command. What is the flag?

THM{g0t-1cmp-p4k3t!}

Once the DNS configuration works fine, resolve the flag.thm.com domain name. What is the IP dress?

172.20.0.120

What is the maximum length for the subdomain name (label)?

63

The Fully Qualified FQDN domain name must not exceed _____ characters.

255

Execute the C2 communication over the DNS protocol of the flag.tunnel.com. What is the flag?

THM{C-TW0-C0MMUN1c4t0ns-0v3r-DN5}

When the iodine connection establishes to Attacker, run the **ifconfig** command.
How many interfaces are? (including the loopback interface)

4

What is the network interface name created by iodined?

dns0

Use the DNS tunneling to prove your access to the webserver,
<http://192.168.0.100/test.php> . What is the flag?

THM{DN5-Tunn311n9-1s-c00l}



Follow

Written by 0xUN7H1NK4BLE

46 Followers · 13 Following

Cyber Security Enthusiast | A learner

No responses yet



What are your thoughts?

Respond

[Open in app](#)**Medium** Search

```
ols>ThreatCheck.exe -f C:\Users\Student\Desktop\Bina
Creating it...
bytes

sing size

sing size
```



0xUN7H1NK4BLE

Signature Evasion : tryhackme

Using the knowledge gained throughout this task, split the binary found in C:\Users\Student\Desktop\Binaries\shell.exe using a native...

Dec 15, 2022  50  2

```
ed.fail!
rator\Desktop/pass-1.txt): No such file or directory in C:\xampp\htdocs\upload-1.php on line 42
```

© 10.10.103.20

THM{koNC473n473_4U_7H3_7H1n95}

OK



0xUN7H1NK4BLE

Obfuscation Principles : Tryhackme Walkthrough

How many core layers make up the Layered Obfuscation Taxonomy?

Dec 14, 2022



53



<code>appendnullbyte.py</code>	Appends the encoded NULL byte character at the end of the payload.
<code>base64encode.py</code>	Base64 all characters in a given payload.
<code>between.py</code>	Replaces greater than operator (>) with NOT BETWEEN 0 AND #.
<code>bluecoat.py</code>	Replaces the space character after an SQL statement with a valid random blank character. Afterward, it replaces the character = with a LIKE operator.
<code>chardoubleencode.py</code>	Double URL—encodes all characters in a given payload (not processing those that are already encoded).
<code>commalesslimit.py</code>	Replaces instances like LIMIT M, N with LIMIT N OFFSET M.
<code>commalessmid.py</code>	Replaces instances like MID(A, B, C) with MID(A FROM B FOR C).
<code>concat2concatws.py</code>	Replaces instances like CONCAT(A, B) with CONCAT_WS(MID(CHAR(0), 0, 0), A, B).
<code>charencode.py</code>	URL—encodes all characters in a given payload (not processing those already



0xUN7H1NK4BLE

SQLmap like a pro...

sqlmap—automatic SQL injection tool

Jan 30, 2023



414



2





0xUN7H1NK4BLE

Data Exfiltration Tips/Tricks

As a security researcher, you have been hired to test the security of a company's network. During your analysis, you discover a...

Mar 24, 2023



55

[See all from 0xUN7H1NK4BLE](#)

Recommended from Medium



Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

★ Sep 7, 2024 🖱 10



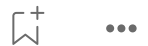


 In T3CH by Axoloth

TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

★ Nov 9, 2024 🖱 100

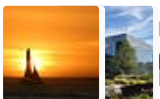


Lists



Staff picks

796 stories · 1561 saves



Stories to Help You Level-Up at Work

19 stories · 912 saves



Self-Improvement 101

20 stories · 3193 saves



Productivity 101


20 stories · 2707 saves



ents

	▼	User Name	▼	Name	▼	Surname	▼	Email
3		student1		Student1				stud
4		student2		Student2				stud
5		student3		Student3				stud
9		anatacker		Ana Tacker				
10		THM(Got.the.User)		X				
11		qweqwe		qweqwe				

<< < 1 > >>

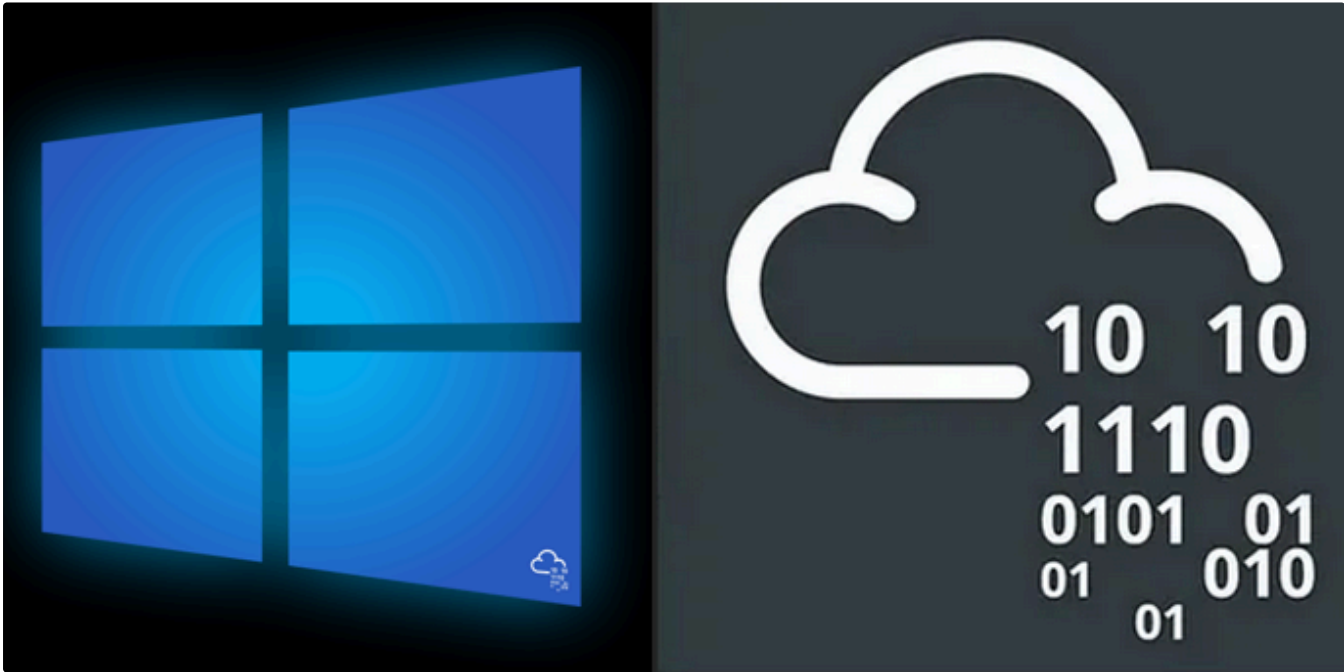
 embossdotar

TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

 Aug 7, 2024  27



 IritT

Windows Fundamentals 1—Complete Beginner—Windows Exploitation Basics—TryHackMe Walkthrough

In part 1 of the Windows Fundamentals module, we'll start our journey learning about the Windows desktop, the NTFS file system, UAC, the...

Oct 23, 2024



In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations



Nov 5, 2024



60



In T3CH by Axoloth

TryHackMe | Search Skills | WriteUp

Learn to efficiently search the Internet and use specialized search engines and technical docs

★ Oct 26, 2024 🖱 61



See more recommendations