TryHackMe | Introduction to Windows API Walkthrough

Trnty · Following

2 min read · Mar 5, 2023

▶ Listen   ⬆ Share   ••• More

Learn how to interact with the win32 API and understand its wide range of use cases

Link- https://tryhackme.com/room/windowsapi

Does a process in the user mode have direct hardware access? (Y/N)

n

Does launching an application as an administrator open the process in kernel mode? (Y/N)

n

What header file imports and defines the User32 DLL and structure?

Open in app ↗

Medium   🔍 Search   🔔   👤

windows.h

What overarching namespace provides P/Invoke to .NET?

system

What memory protection solution obscures the process of importing API calls?

aslr

Which character appended to an API call represents an ANSI encoding?

a

Which character appended to an API call represents extended functionality?

ex

Keshribhan, read the best stories from industry leaders on Medium.

The author made this story available to Medium members only. Upgrade to instantly unlock this story plus other member-only benefits.

✦ Access all member-only stories on Medium

✦ Become an expert in your areas of interest

✦ Get in-depth answers to thousands of questions about technical

✦ Grow your career or build a new one

Marc-André Giroux
Sr. Software Developer
Netflix

Carlos Arguelles
Sr. Staff Engineer
Google

Tony Yiu
Director
Nasdaq

Brandeis Marshall
CEO
DataedX

Cassie Kozyrkov
Chief Decision Scientist
Google

Memo Akten
Asst. Professor
UCSD

Vitali Zaidman
Software Architect
Meta

Camille Fournier
Head of Engineering
JPMorgan Chase

Upgrade

Following

Written by Trnty

543 Followers · 0 Following

Blue Team Cyber Defender | Check out https://blueteamcyberdefender1.blogspot.com for newer articles !

No responses yet

What are your thoughts?

Respond

More from Trnty

Trnty

TryHackMe | Red Team Engagements WriteUp

Learn the steps and procedures of a red team engagement, including planning, frameworks, and documentation.

May 3, 2022   ✋ 13

Trnty

TryHackMe | Red Team Fundamentals WriteUp

This room is an introduction to red teaming

👤 Trnty

TryHackMe | Preparation Walkthrough

A look into the Preparation phase of the Incident Response.

```
on 10.0.14393]
ration. All rights reserved.

oles>"c:\Program Files\ClamAV\sigtool.exe
07ab3a88:6144:AV-Check.exe

oles>_
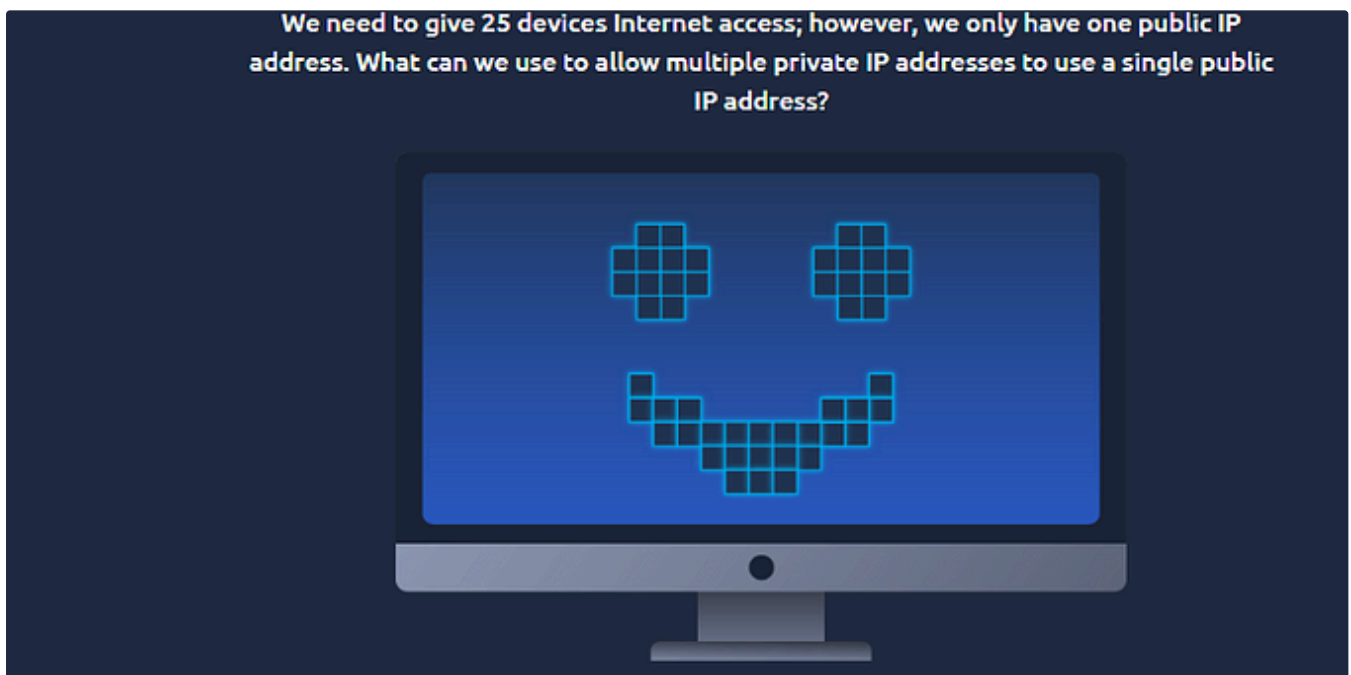```

👤 Trnty

## TryHackMe | Introduction to Antivirus WriteUp

Understand how antivirus software works and what detection techniques are used to bypass malicious files checks.

✦ Jun 25, 2023 👏 4 🔖⁺ •••

---

See all from Trnty

---

# Recommended from Medium



✅ embossdotar

## TryHackMe — Networking Essentials — Writeup

Key points: Networking protocols | DHCP | ARP | NAT | ICMP | Ping | Traceroute. Networking Essentials by awesome TryHackMe! 🎉

✦ Oct 22, 2024 👏 1 🔖⁺ •••

---

rutbar

# TryHackMe — Search Skills | Cyber Security 101 (THM)

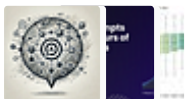Evaluation of Search Results

✦    Oct 26, 2024    💬 1

---

## Lists
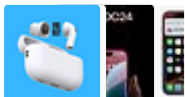

### AI Regulation
6 stories  ·  670 saves


### ChatGPT prompts
51 stories  ·  2477 saves


### Tech & Tools
22 stories  ·  387 saves


### Generative AI Recommended Reading
52 stories  ·  1602 saves

---

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

| ommand | Explanation |
|---|---|
| `cpdump -i INTERFACE` | Captures packets on a specific network interface |
| `cpdump -w FILE` | Writes captured packets to a file |
| `cpdump -r FILE` | Reads captured packets from a file |
| `cpdump -c COUNT` | Captures a specific number of packets |
| `cpdump -n` | Don't resolve IP addresses |
| `cpdump -nn` | Don't resolve IP addresses or protocol numbers |
| `cpdump -v` | Verbose display; increase with `-vv` and `-vvv` |

rutbar

# TryHackMe — Tcpdump: The Basics | Cyber Security 101 (THM)

Introduction

⭐    Oct 23, 2024    ✋ 6

erative that we understand and can protect against common attacks.
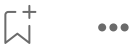
mon techniques used by attackers to target people online. It will also teach some of the best wa

Daniel Schwarzentraub

# Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

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 | | |

✓ embossdotar

# TryHackMe — Session Management — Writeup

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

See more recommendations