

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



Introduction to Windows API TryHackMe



Avataris12 · [Follow](#)

2 min read · Sep 5, 2022



Listen



Share

... More

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

Subsystem and Hardware Interaction

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

Components of the Windows API

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

winuser.h

What parent header file contains all other required child and core header files?

windows.h

OS Libraries

What overarching namespace provides P/Invoke to .NET?

system

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

ASLR

API Call Structure

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

A

Which character appended to an API call represents extended functionality?

Ex

What is the memory allocation type of 0x00080000 in the VirtualAlloc API call?

<https://docs.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-virtualalloc>

MEM_RESET

C API Implementations

Do you need to define a structure to use API calls in C? (Y/N)

N

.NET and PowerShell API Implementations

What method is used to import a required DLL?

DllImport

What type of method is used to reference the API call to obtain a struct?

External

Commonly Abused API Calls

Which API call returns the address of an exported DLL function?

GetProcAddress

Which API call imports a specified DLL into the address space of the calling process?

LoadLibrary

Malware Case Study

What Win32 API call is used to obtain a pseudo handle of our current process in the keylogger sample?

GetCurrentProcess

What Win32 API call is used to set a hook on our current process in the keylogger sample?

SetWindowsHookEx

What Win32 API call is used to obtain a handle from the pseudo handle in the keylogger sample?

GetModuleHandle

What Win32 API call is used to unset the hook on our current process in the keylogger sample?

UnhookWindowsHookEx

What Win32 API call is used to allocate memory for the size of the shellcode in the shellcode launcher sample?

VirtualAlloc

What native method is used to write shellcode to an allocated section of memory in the shellcode launcher sample?

Marshal.Copy

What Win32 API call is used to create a new execution thread in the shellcode launcher sample?

CreateThread

What Win32 API call is used to wait for the thread to exit in the shellcode launcher sample?

WaitForSingleObject

Support me as a writer by signing up for a Medium membership with my [referral link](#), which gives you access to all my posts (and everyone else's on Medium) →

Join Medium with my referral link — Avataris12

Read every story from Avataris12 (and thousands of other writers on Medium). Your membership fee directly supports...

medium.com

Tryhackme Walkthrough

Tryhackme

Tryhackme Writeup

Windows

Malware



Follow

Open in app ↗

Medium



Search



Cybersecurity enthusiast

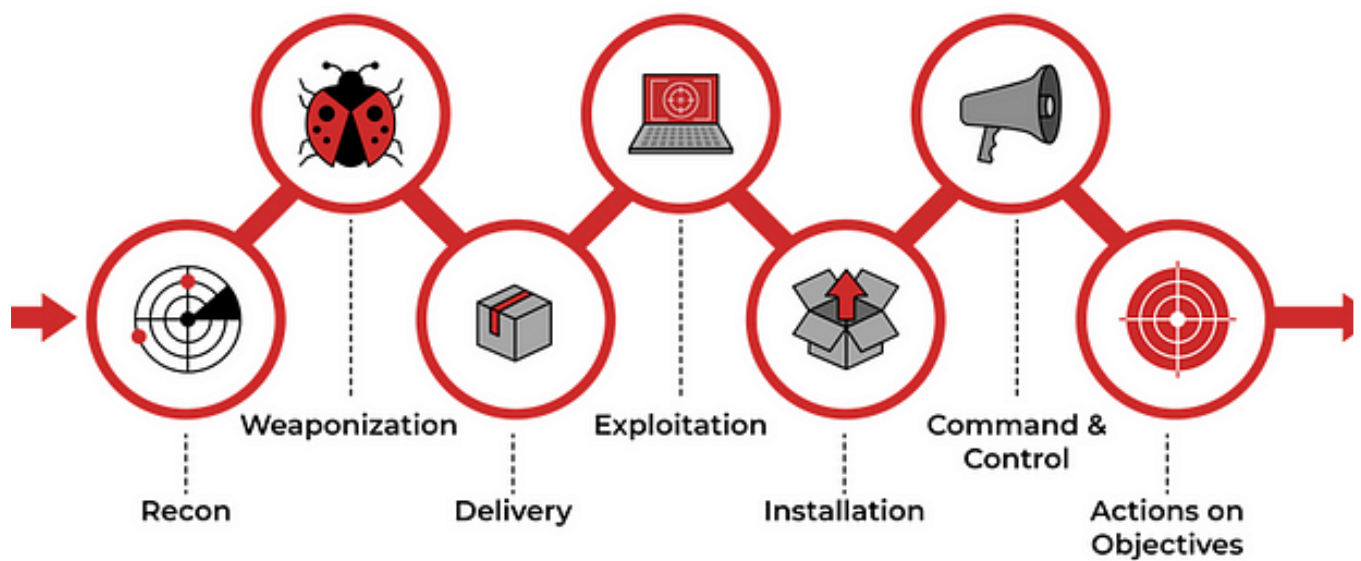
No responses yet



What are your thoughts?

Respond

More from Avataris12



Avataris12

Cyber Kill Chain TryHackMe

Reconnaissance

★ Sep 14, 2022 🖱 20



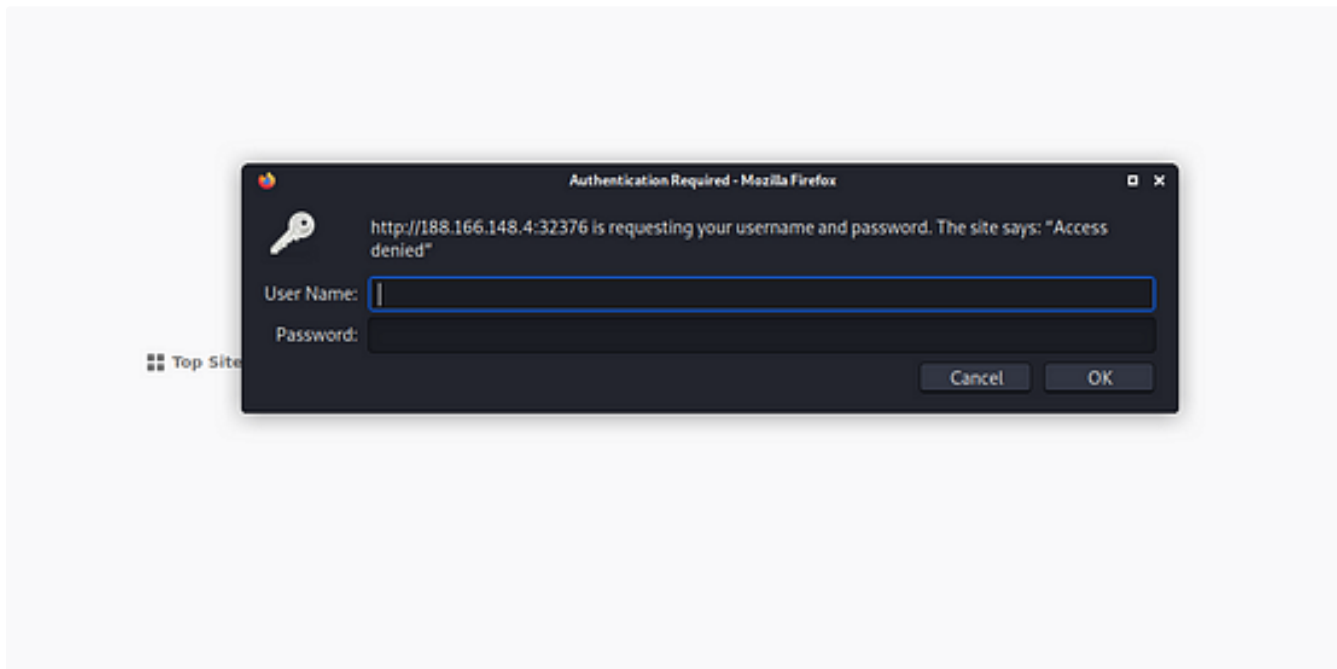


 Avataris12

Intro to Network Traffic Analysis

Networking Primer — Layers 1–4

Aug 8, 2022  6



 Avataris12

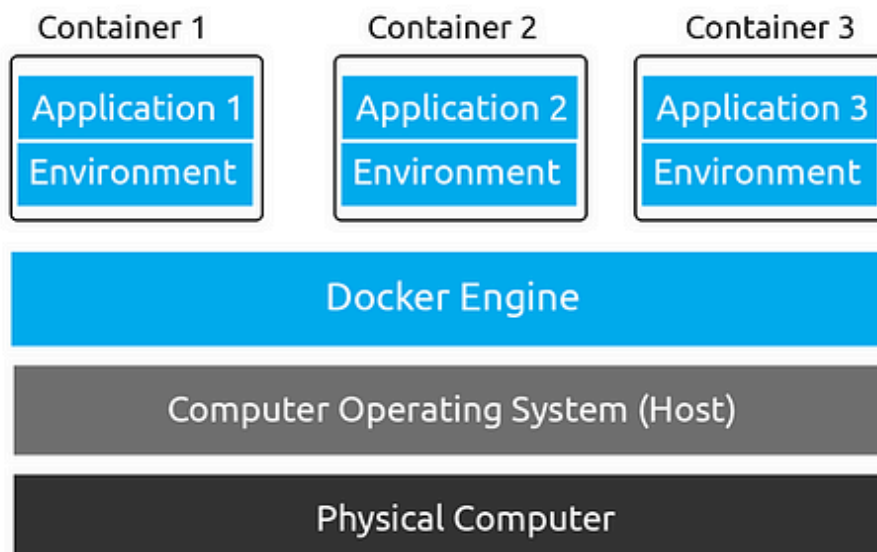
HTB Login Brute Forcing

Default Passwords

Mar 21, 2022  10



A diagram demonstrating three containers
on a single computer



Avataris12

Intro to Containerisation TryHackMe

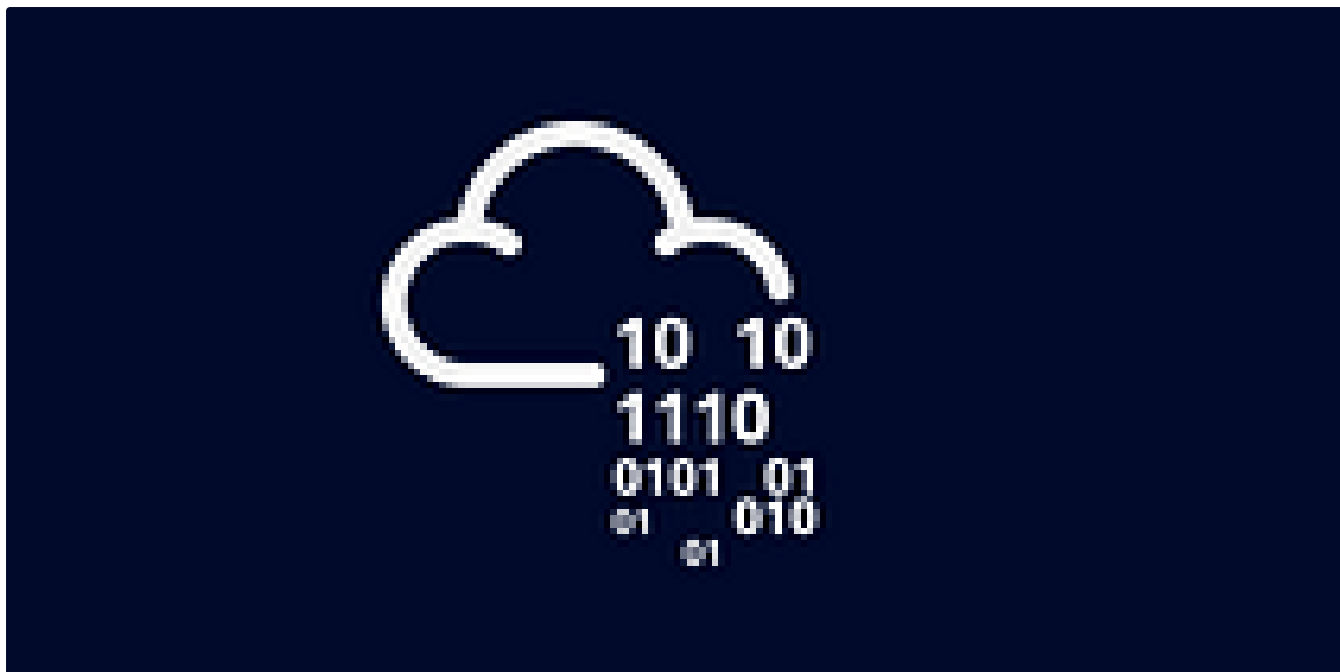
<https://tryhackme.com/room/introtocontainerisation>

★ Dec 1, 2022 🖱 19



See all from Avataris12

Recommended from Medium



In T3CH by Axoloth

TryHackMe | AD Certificate Templates | WriteUp

Walkthrough on the exploitation of misconfigured AD certificate templates



Sep 11, 2024



70



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



rutbar

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

Introduction



Oct 23, 2024



6



Lists



Staff picks

800 stories · 1569 saves



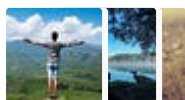
Stories to Help You Level-Up at Work

19 stories · 920 saves



Self-Improvement 101

20 stories · 3227 saves



Productivity 101

20 stories · 2726 saves



Day 11
Answers

cyberw1ng.medium.com

 In System Weakness by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 11] Writeup with Answers | TryHackMe Walkthrough

If you'd like to WPA, press the star key!


★ Dec 11, 2024 🖱 855 💬 1



ints

	User Name	Name	Surname	Email
3	student1	Student1		stud1
4	student2	Student2		stud2
5	student3	Student3		stud3
9	anatacker	Ana Tacker		
10	THM (Got the User)	X		
11	qwerty	qwerty		

40 0 1 0 00

 embossdotar

TryHackMe—Session Management—Writeup

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

★ Aug 7, 2024 🖱 27



erative that we understand and can protect against common attacks.

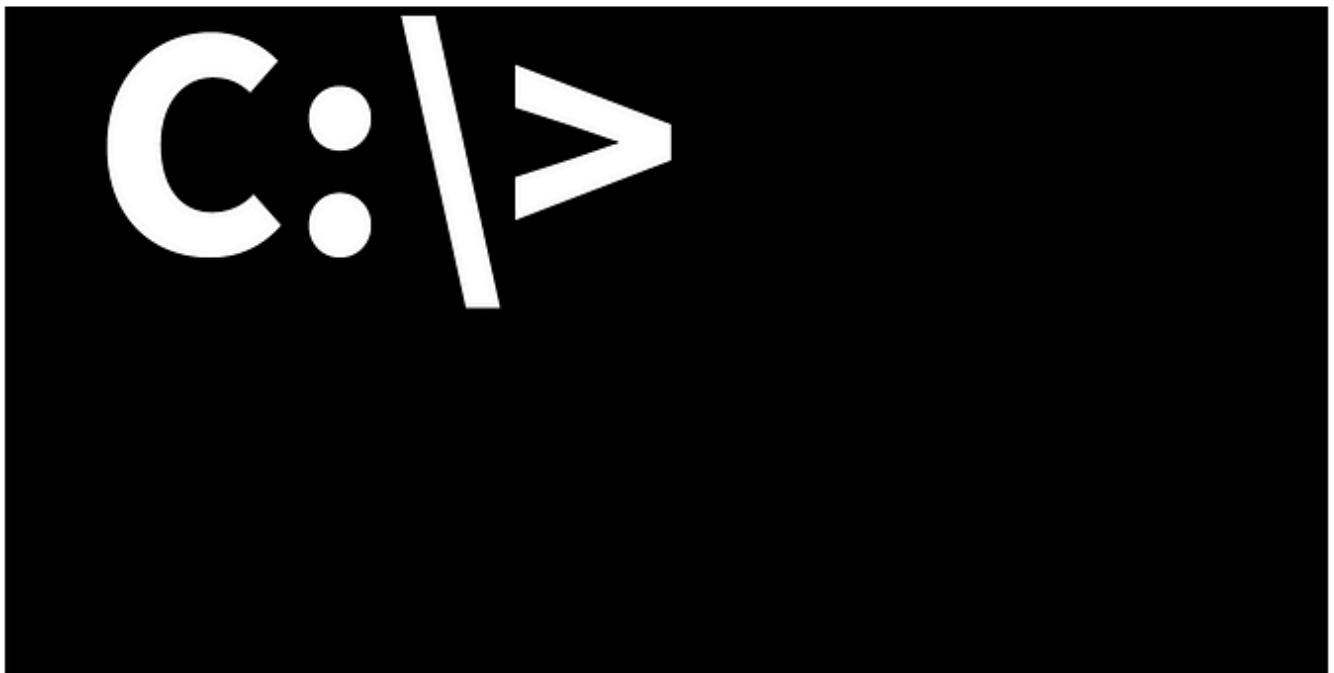
mon techniques used by attackers to target people online. It will also teach some of the best way

 Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024



In System Weakness by Sunny Singh Verma [SuNnY]

Windows Command Line [CyberSecurity 101 Learning Path] TryHackMe Writeup | Detailed Walkthrough |...

Windows Command Line is a Part of The Learning Path From the Newly updated Cyber Security 101 Path on TryHackMe

Oct 26, 2024  67



See more recommendations