




ENDPOINT SECURITY

CHRISTOPHER HENSHAW


30342470






DashboardLearnPracticeCompete

SearchNotifications22Profile



christopherhenshaw@students.federation.edu.au

Student ID: 30342470 


Add Socials

Get profile badge ID


Share room badges

0 Following0 Followers


Rank

 443822


Badges

 4

Streak

 22

Completed rooms

 21



Intro to Endpoint Security

Learn about fundamentals, methodology, and tooling for endpoint security monitoring.

  60 min  74,113 



TRYHACKME

ENDPOINT SECURITY: WHERE THE WAR BEGINS, AND
LESSONS ARE EARNED.





THE TOOLS OF THE TRADE:

TCPView

Process Explorer

Sysmon

OSQuery

Instructions: Identify the abnormal running process. You may open the Baseline Document created by the security team.

Baselined Processes.docx

Proc

wininit.exe
csrss.exe
svchost.exe
beacon.exe

csrss.exe
smss.exe
wininit.exe
winlogon.exe
explorer.exe
svchost.exe

winlogon.exe	6.0%	69.6 Mb	0.3 MB/s
explorer.exe	4.3%	69.9 Mb	0.0 MB/s
smss.exe	11.4%	39.4 Mb	0.3 MB/s

THE DISCOVERY



Type here to search



1.
5

Notes

Malicious process:
beacon.exe

Instruction: Based on the identified malicious process, determine the malicious network traffic. You may refer to your notes.

Process Name	Process ID	Remote Address	Remote Port
svchost.exe	2031	time.windows.com	443
svchost.exe	1023	52.242.211.89	443
beacon.exe	6823	59.23.48.195	4444

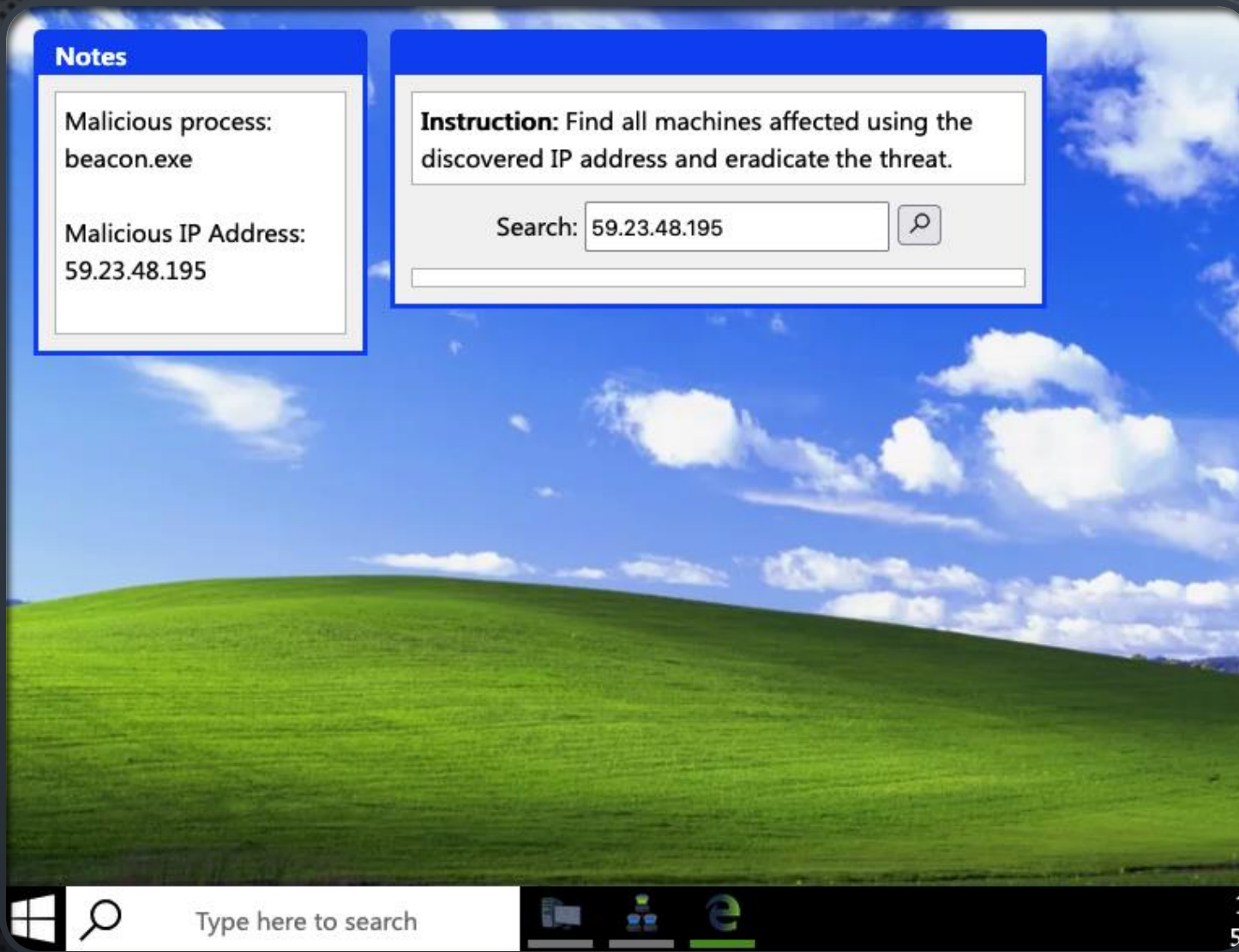
PORT 4444



Type here to search



14:01 PM
5/10/2025



THE TRAIL

Notes

Malicious process:
beacon.exe

Malicious IP Address:
59.23.48.195

Instruction: Find all machines affected using the discovered IP address and eradicate the threat.

Search: 59.23.48.195



Computer Name	Remote IP Address	Action
WKSTN-1	59.23.48.195	Remediate
WKSTN-2	59.23.48.195	Remediate
WKSTN-3	59.23.48.195	Remediate
WKSTN-4	59.23.48.195	Remediate



Congratulations! You have successfully eradicated the threat. You may get your reward from the flag.txt file on the Desktop

SYSTEM INTEGRITY



You did it! 🎉 Intro to Endpoint Security complete!

Points earned

🎯 48

Completed tasks

☑️ 5

Room type

🧑 Walkthrough

Difficulty

📶 Easy

Streak

🔥 19



77,892 users are actively learning this week



FINAL REFLECTION



Thank You





REFERENCES

- TRYHACKME
- ADOBE STOCK PHOTOGRAPHS

The background is a dark, textured surface with a fine halftone dot pattern. Overlaid on this are several large, semi-transparent, light-gray geometric shapes, including circles and polygons, which are arranged in a way that suggests a complex, layered composition. The word "QUESTIONS?" is centered in a white, sans-serif font.

QUESTIONS?