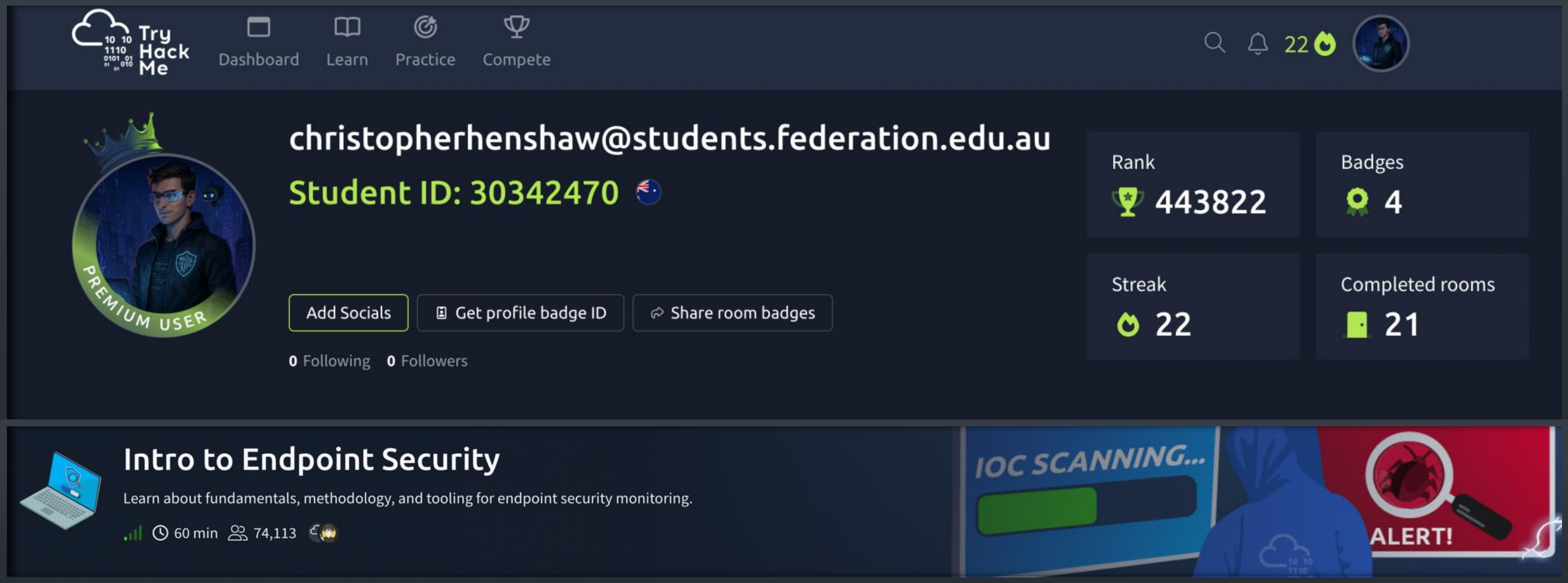
ENDPOINT SECURITY

CHRISTOPHER HENSHAW

30342470



christopherhenshaw@students.federation.edu.au

Student ID: 30342470

0 Following 0 Followers

Rank 443822

Badges 4

Streak 22

Completed rooms 21

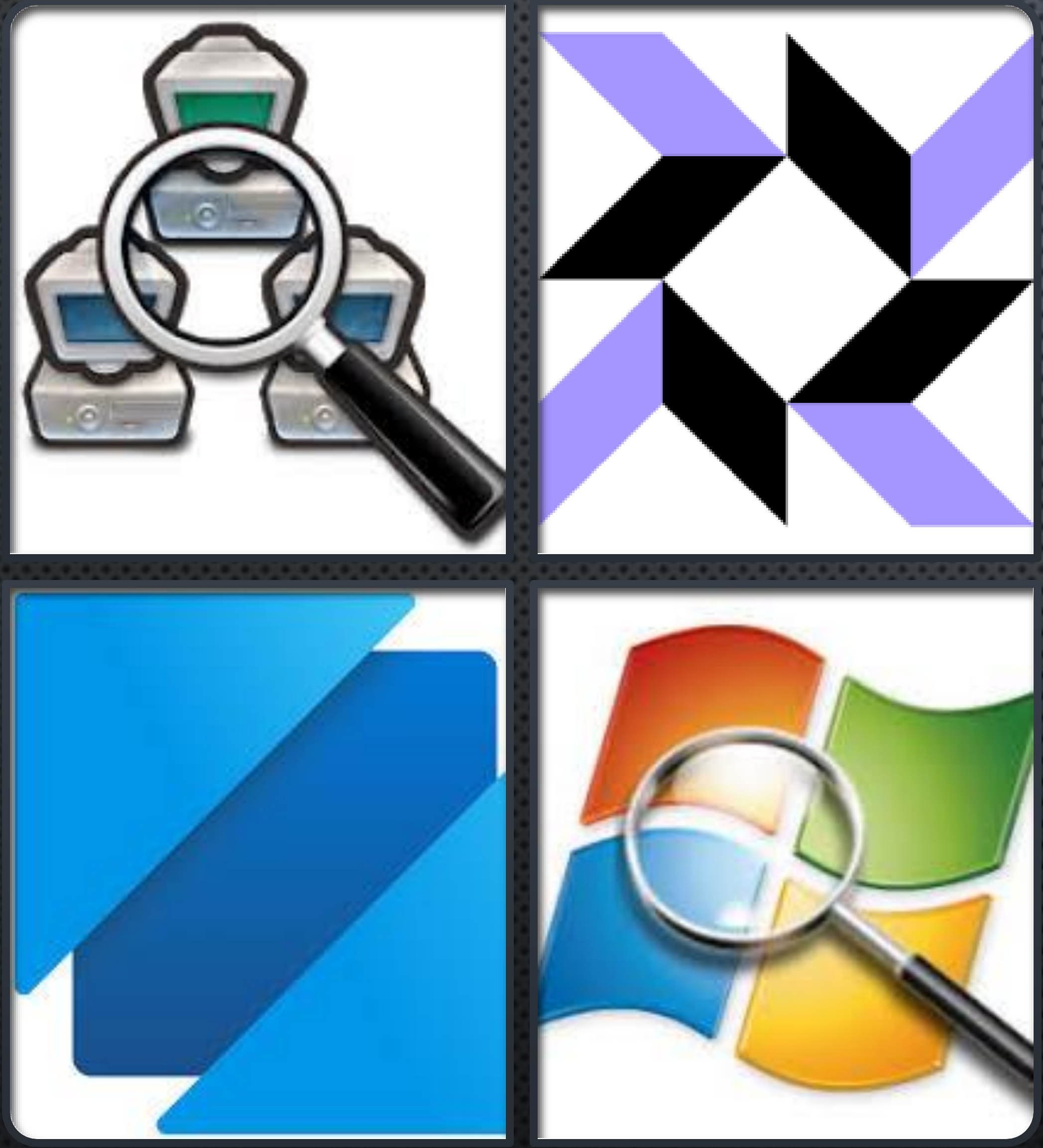
Intro to Endpoint Security

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

60 min 74,113

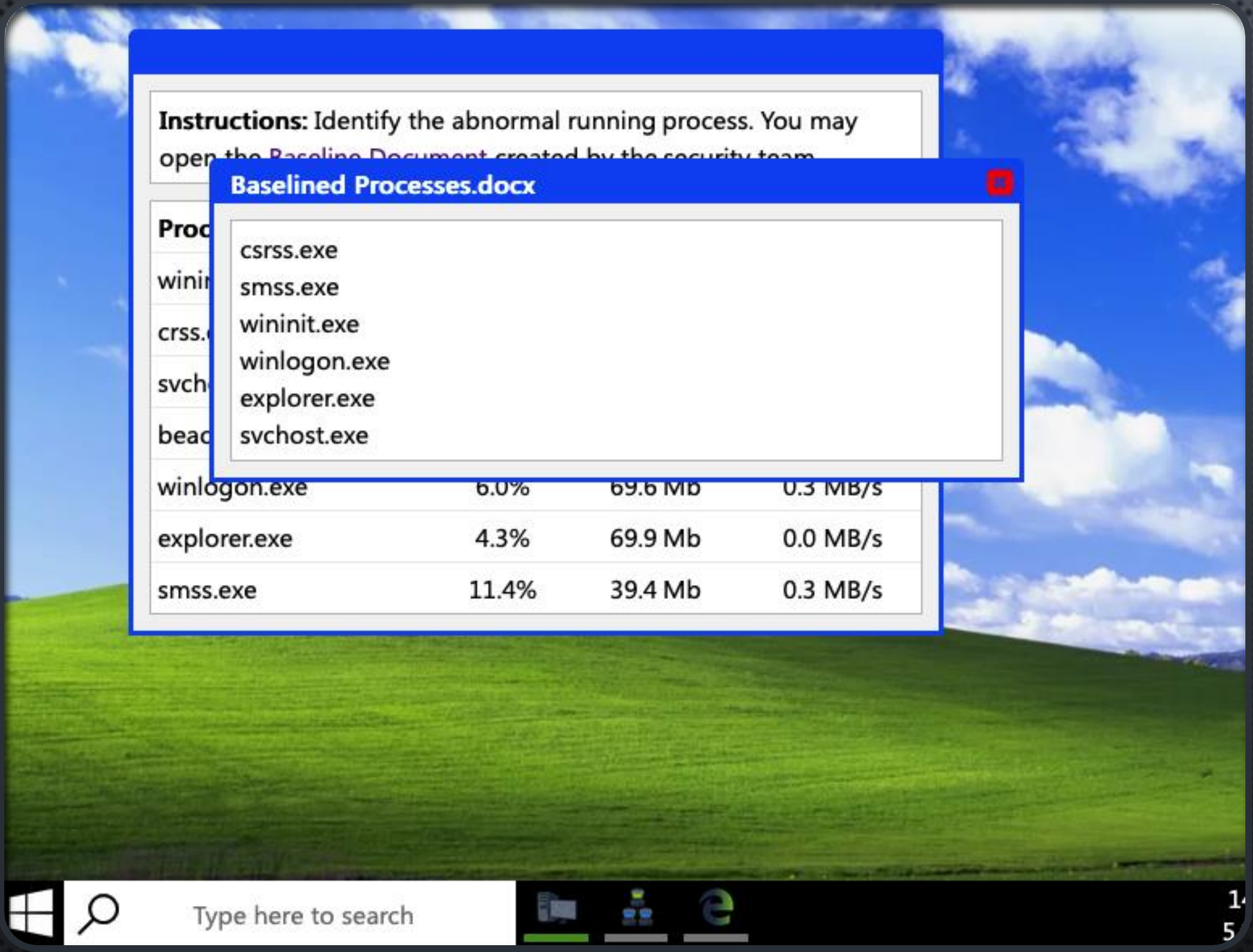
TRYHACKME

Endpoint Security: where the war begins, and lessons are earned.



THE TOOLS OF THE TRADE:

- TCPView
- Process Explorer
- Sysmon
- OSQuery



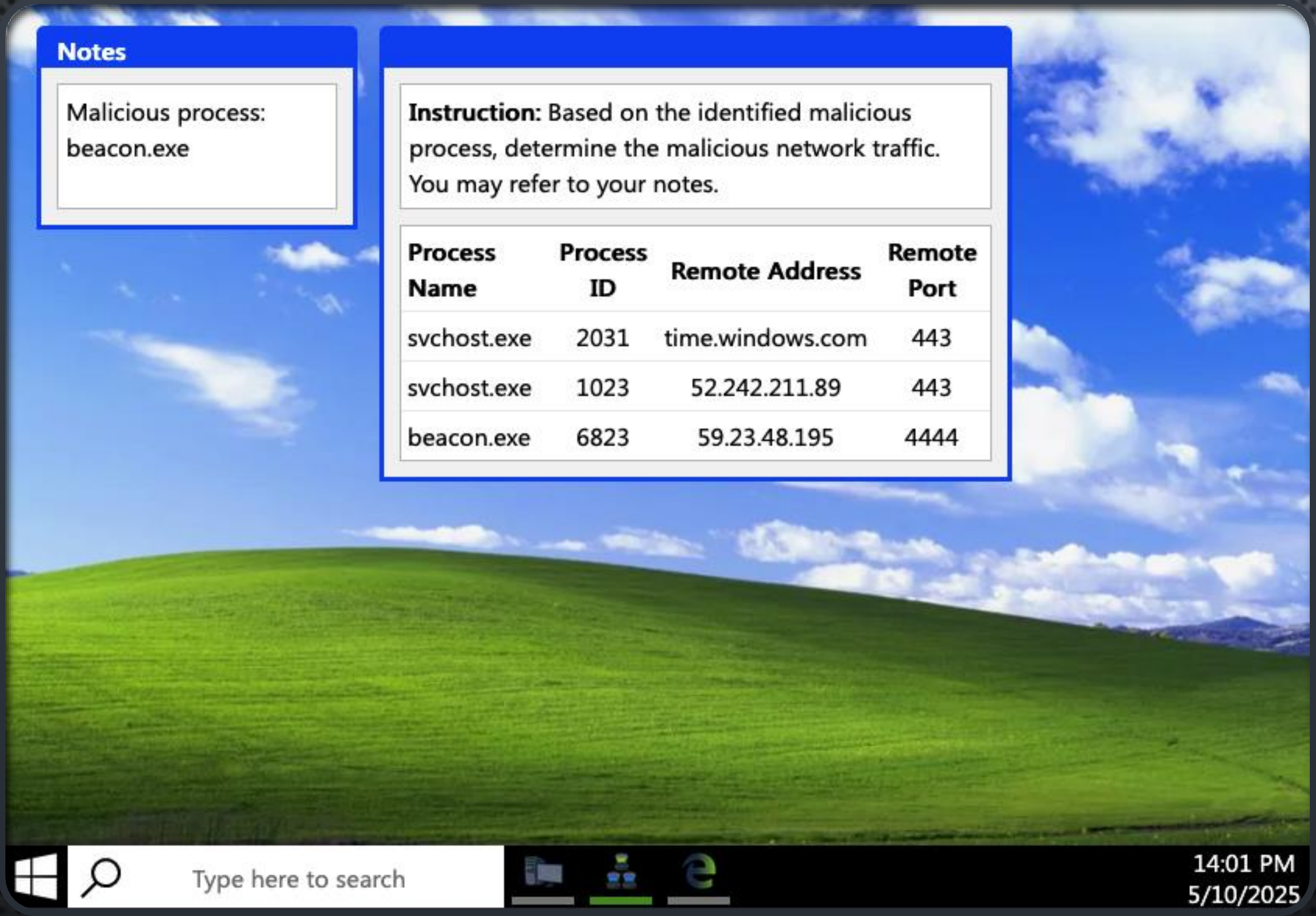
Instructions: Identify the abnormal running process. You may open the Baseline Document created by the security team.

Proc			
winir			
crss.			
svch			
beac			
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

Baselined Processes.docx

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

THE DISCOVERY



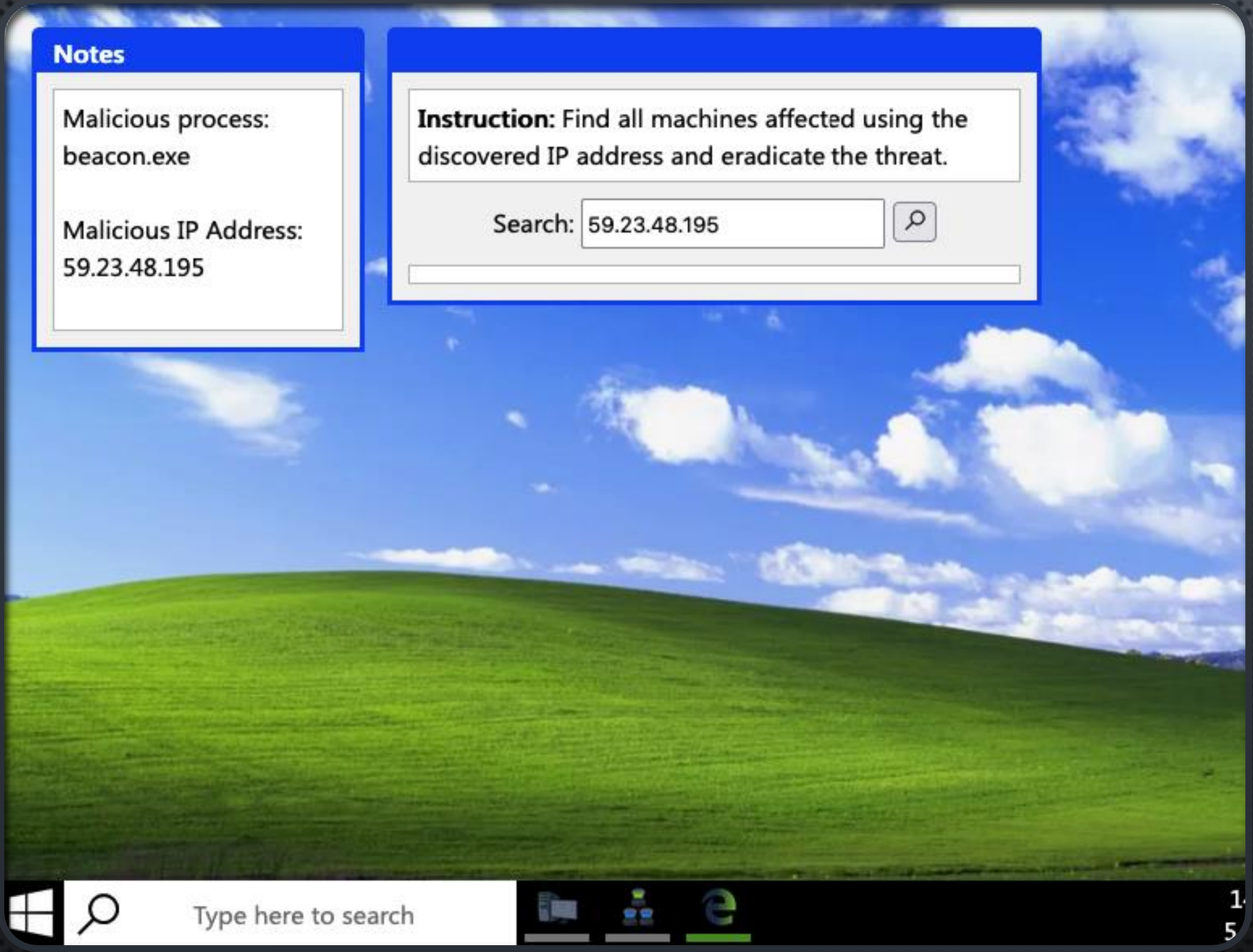
Malicious process:
beacon.exe

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

THE TRAIL



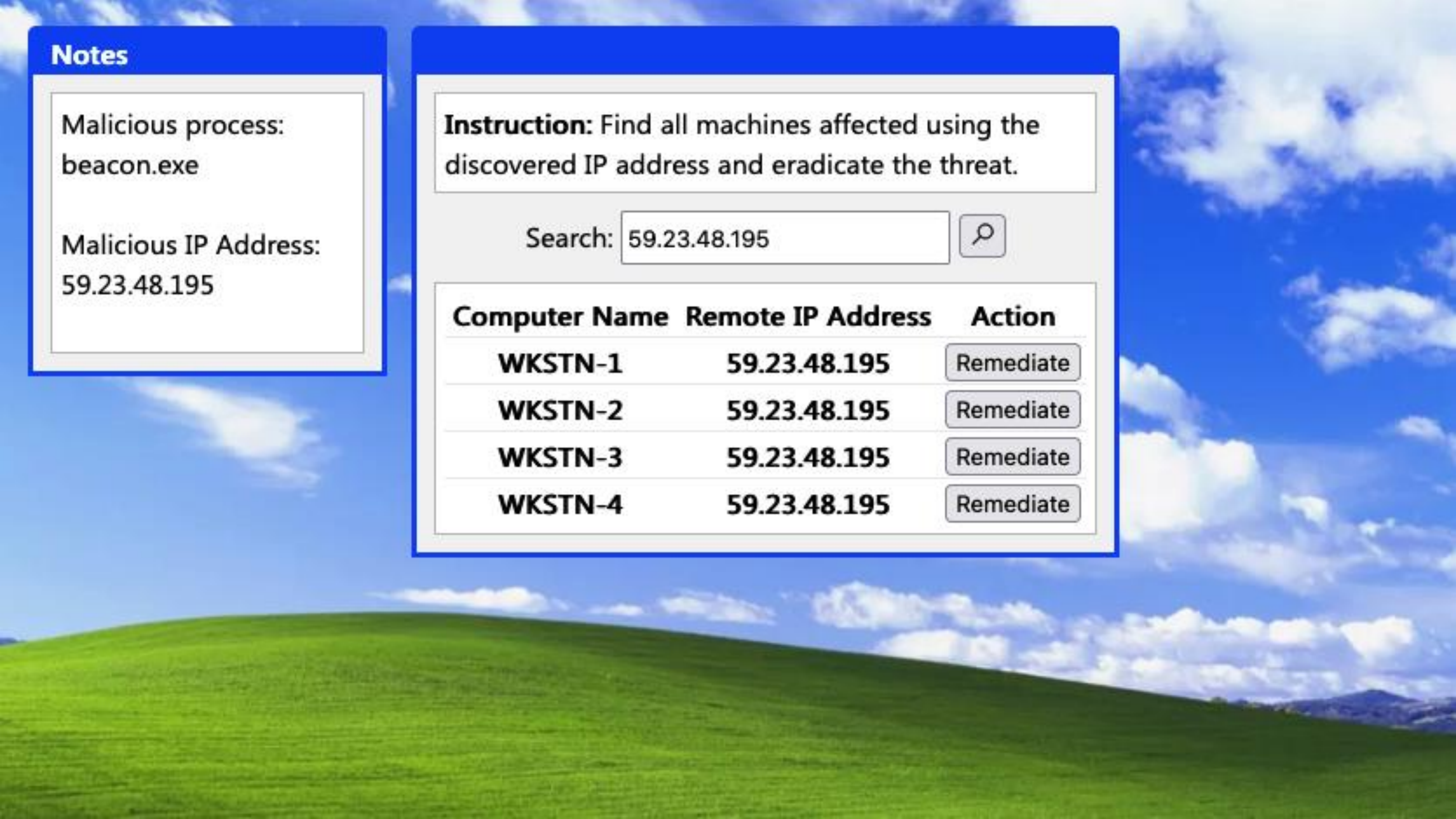
Notes

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



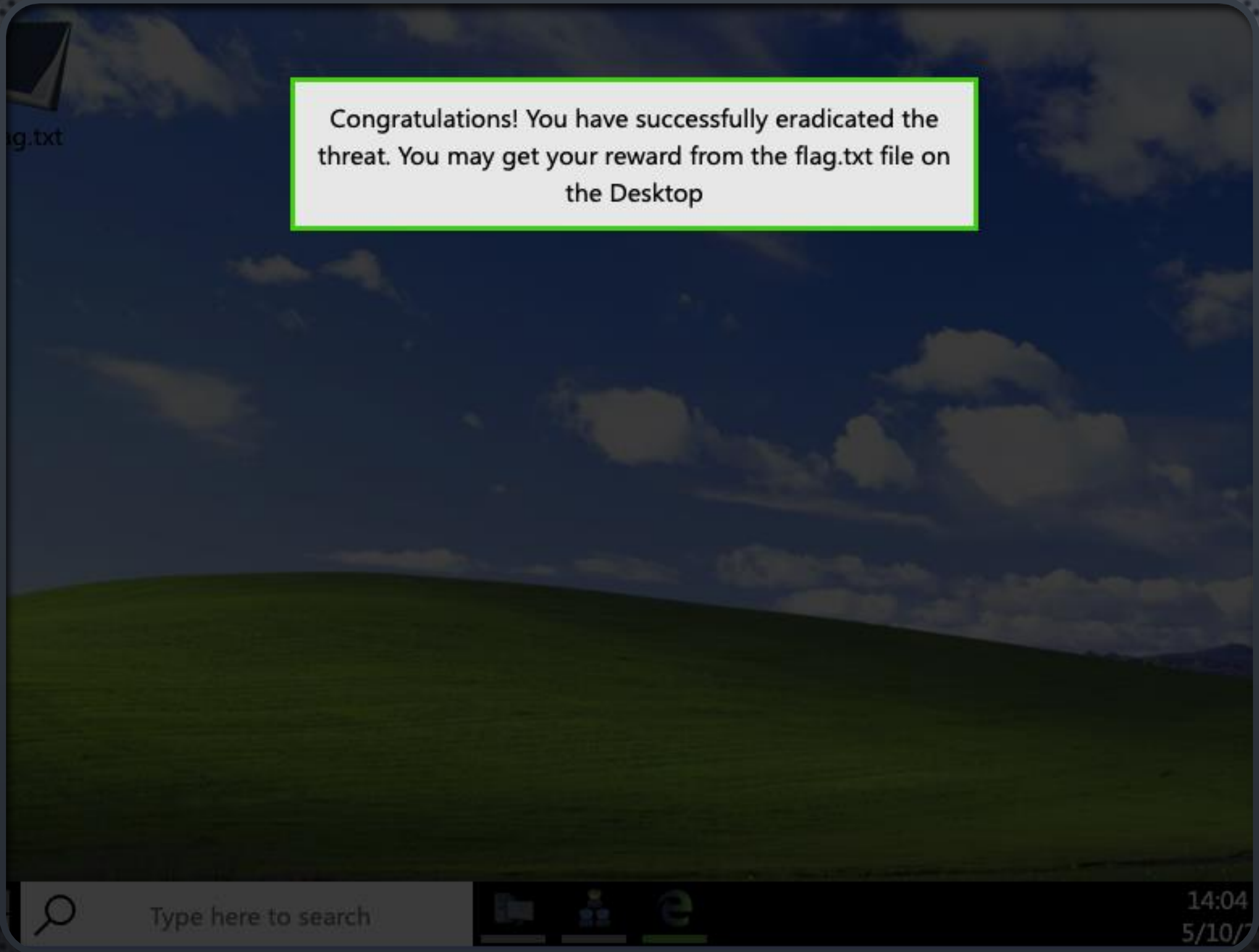
Malicious process:
beacon.exe

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	Completed tasks	Room type	Difficulty	Streak
48	5	Walkthrough	Easy	19

77,892 users are actively learning this week

FINAL REFLECTION

Thank You

References

- TryHackMe
- Adobe Stock Photographs

QUESTIONS?