Mission Name

The Backdoor

Historical Context

Ethan has identified unauthorized access on his computer, experiencing the irony of a hacker being hacked. His current objective is to locate the intruder and sever their connection.

Overview of Technical Strategy

Upon discovering unauthorized access to his computer, Ethan's priority is to uncover the concealed backdoor and eliminate it from his system.

Brief Mission Overview

Your computer has been compromised with a backdoor, putting you under surveillance. Your mission is to locate and eradicate this security threat. Best of luck!

Detailed Mission Brief

Ethan finds himself in a precarious situation with unauthorized access discovered on his computer— a hacker facing the brunt of hacking. He is now on a quest to identify the intruder and disrupt their communications.

Operational Venue

ANTUM | HAB BLOCK DISTRICT | ETHAN'S APARTMENT

Tools

- User: ethan
- Password: Myp4ssw0rd

Questions

What is the name of the .exe used to launch the backdoor?

- Utilman.exe

What is the full path of modified registry?

- HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe

What is the item of the modified registry changed?

- Debugger

Items

- Search for changes in registry
- Check the registry key: HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe
- Lock the session.

Categories

Windows
Enumeration
Backdoor

Write Up

Gain entry to the system and reviewing the system registry reveals alterations to the Utilman.exe key:

- `HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe`

- Secure the session.

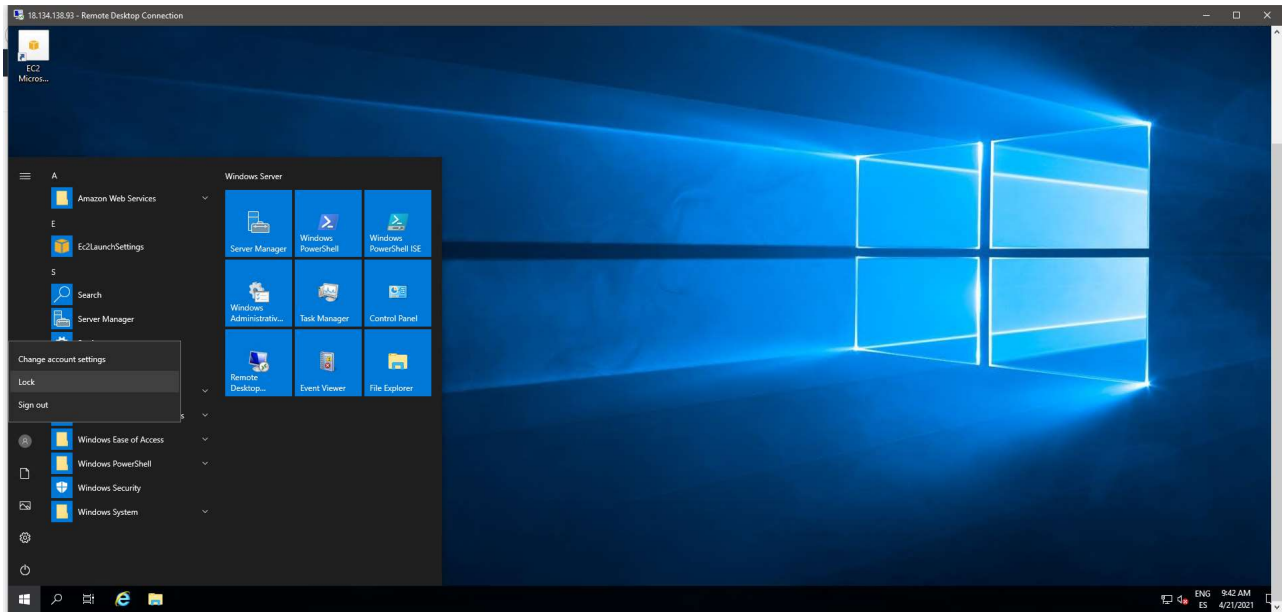

Figure 1

Select the bottom right corner to open a command prompt with administrator privileges.

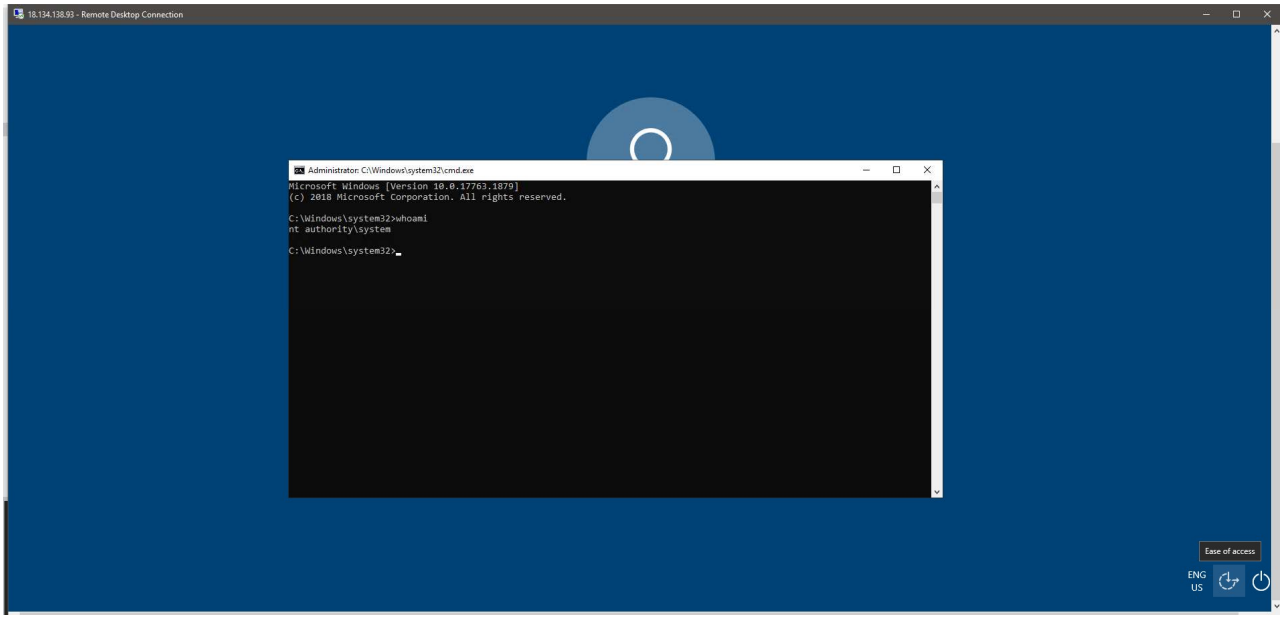

Figure 2

Retrieve the flag located on the administrator's desktop.

Flag Information

flag{w0w_th4s_was_an_0ld_tr1ck}