Microsoft Windows Hardening

Task-1
No answer needed

Task-2
What is the startup type of App Readiness service in the services panel?
manual

Open Registry Editor and find the key “tryhackme”. What is the default value of the key?
{THM_REG_FLAG}

Open the Diagnosis folder and go through the various log files. Can you find the flag?
{THM_1000710}

Task-3
Find the name of the Administrator Account of the attached VM.
Harden

Go to the User Account Control Setting Panel (Control Panel > All Control Panel Items > User Accounts). What is the default level of Notification?
Always notify

How many standard accounts are created in the VM?
0

Task-4
Open Windows Firewall and click on Monitoring in the left pane - which of the following profiles is active? Domain, Private, Public?
private

Find the IP address resolved for the website tryhack.me in the Virtual Machine as per the local hosts file.
192.168.1.140

Open the command prompt and enter arp -a. What is the Physical address for the IP address 255.255.255.255?
ff-ff-ff-ff-ff-ff

Task-5
Windows Defender Antivirus is configured to exclude a particular extension from scanning. What is the extension?
.ps

A Word document is received from an unknown email address. It is best practice to open it immediately on your personal computer (yay/nay).
nay

What is the flag you received after executing the Office Hardening Batch file?
{THM_1101110}

Task-6
A security engineer has misconfigured the attached VM and stored a BitLocker recovery key in the same computer. Can you read the last six digits of the recovery key?
377564

How many characters does the BitLocker recovery key have in the attached VM?
48

A backup file is placed on the Desktop of the attached VM. What is the extension of that file?
.bkf

Task-7
What is the CVE score for the vulnerability CVE ID CVE-2022-32230?
7.8

Task-8
No answer needed