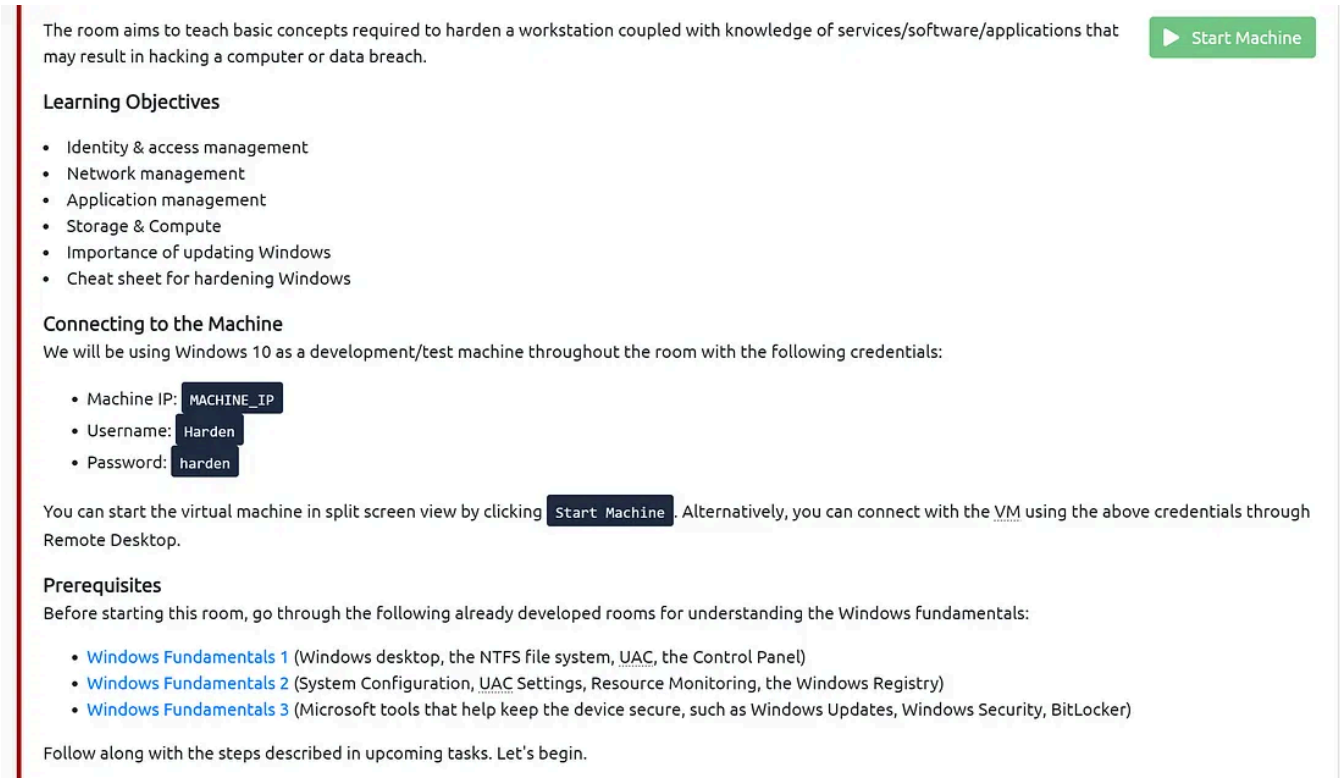
# Tryhackme: Microsoft Windows Hardening

Daniel Schwarzentraub · Follow
5 min read · Sep 28, 2023



## Task 1: Introduction



The room aims to teach basic concepts required to harden a workstation coupled with knowledge of services/software/applications that may result in hacking a computer or data breach.

Start Machine

**Learning Objectives**

- Identity & access management
- Network management
- Application management
- Storage & Compute
- Importance of updating Windows
- Cheat sheet for hardening Windows

**Connecting to the Machine**

We will be using Windows 10 as a development/test machine throughout the room with the following credentials:

- Machine IP: `MACHINE_IP`
- Username: `Harden`
- Password: `harden`

You can start the virtual machine in split screen view by clicking `Start Machine`. Alternatively, you can connect with the VM using the above credentials through Remote Desktop.

**Prerequisites**

Before starting this room, go through the following already developed rooms for understanding the Windows fundamentals:

- Windows Fundamentals 1 (Windows desktop, the NTFS file system, UAC, the Control Panel)
- Windows Fundamentals 2 (System Configuration, UAC Settings, Resource Monitoring, the Windows Registry)
- Windows Fundamentals 3 (Microsoft tools that help keep the device secure, such as Windows Updates, Windows Security, BitLocker)

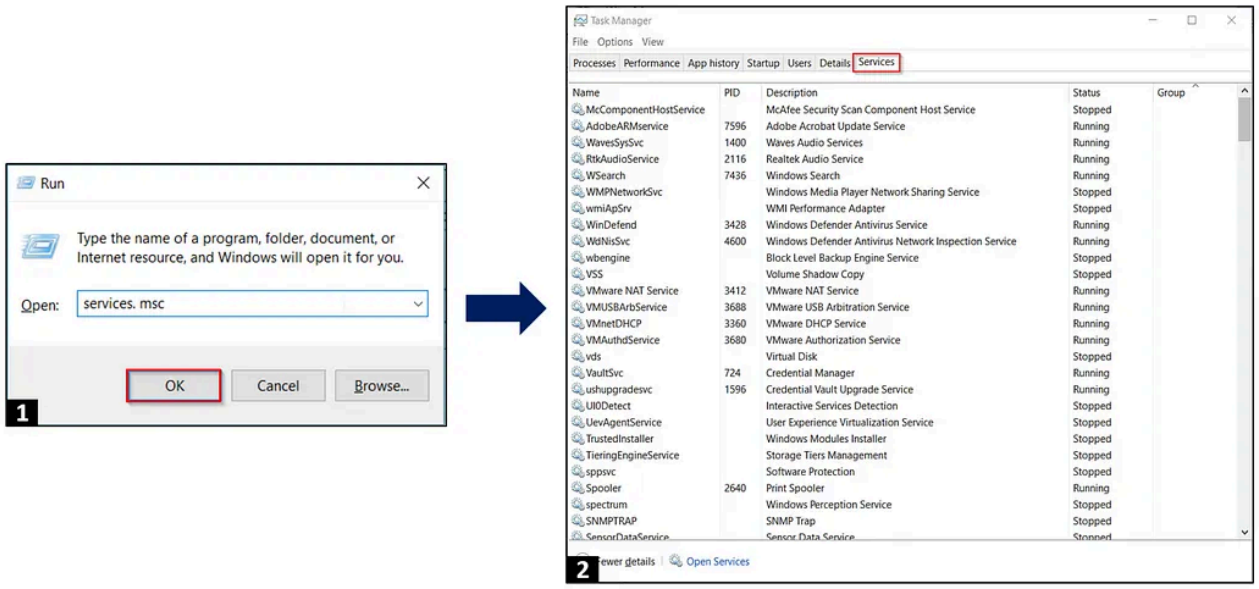
Follow along with the steps described in upcoming tasks. Let's begin.

## Task 2: Understanding General Concepts

### Services

Windows Services create and manage critical functions such as network connectivity, storage, memory, sound, user credentials, and data backup and runs automatically in the background. These services are managed by the Service Control Manager panel and divided into three categories, i.e. Local, Network & System. Many applications like browsers and anti-virus software can also run their services for a seamless user experience.

Type `services.msc` in the Run window to access Windows services.

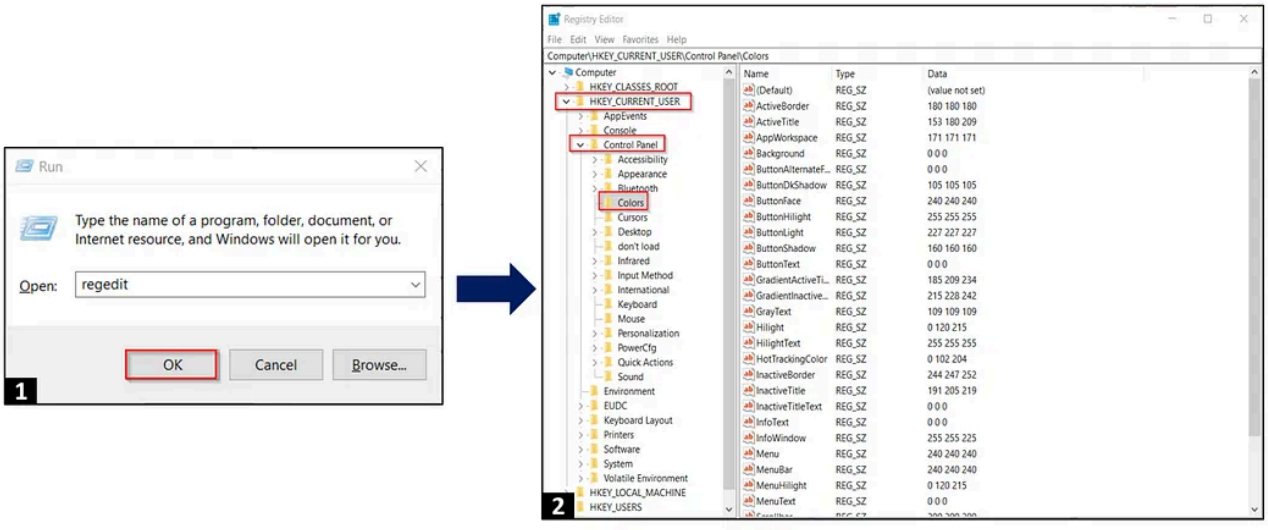



### Windows Registry

The Windows registry is a unified container database that stores configurational settings, essential keys and shared preferences for Windows and third-party applications. Usually, on the installation of most applications, it uses a registry editor for storing various states of the application. For example, suppose an application (malicious or normal) wants to execute itself during the computer boot-up process; In that case, it will store its entry in the Run & Run Once key.

Usually, a malicious program makes undesired changes in the registry editor and tries to abuse its program or service as part of system routine activities. It is always recommended to protect the registry editor by limiting its access to unauthorised users.

Type `regedit` in the Run dialogue or taskbar search to access the registry editor.



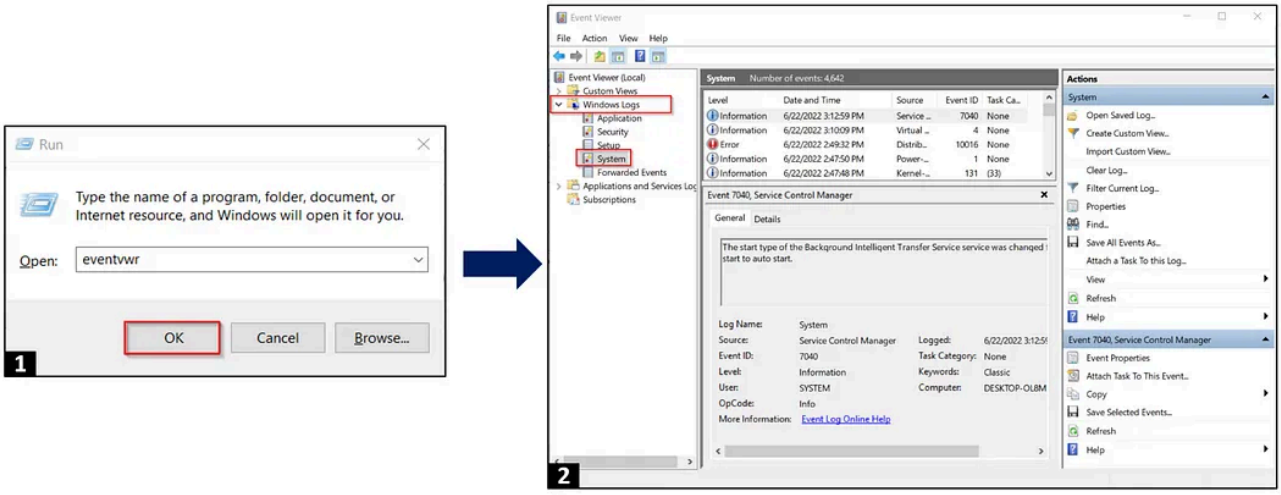
### Event Viewer

Event Viewer is an app that shows log details about all events occurring on your computer, including driver updates, hardware failures, changes in the operating system, invalid authentication attempts and application crash logs. Event Viewer receives notifications from different services and applications running on the computer and stores them in a centralised database.

Hackers and malicious actors access Event Viewer to increase their attack surface and enhance the target system's profiling. Event categories are as below:

- **Application**: Records events of already installed programs.
- **System**: Records events of system components.
- **Security**: Logs events related to security and authentication etc.

We can access Event Viewer by typing `eventvwr` in the Run window. The default location for storing events is `C:\WINDOWS\system32\config\folder` in the attached VM (`10.10.175.97`).

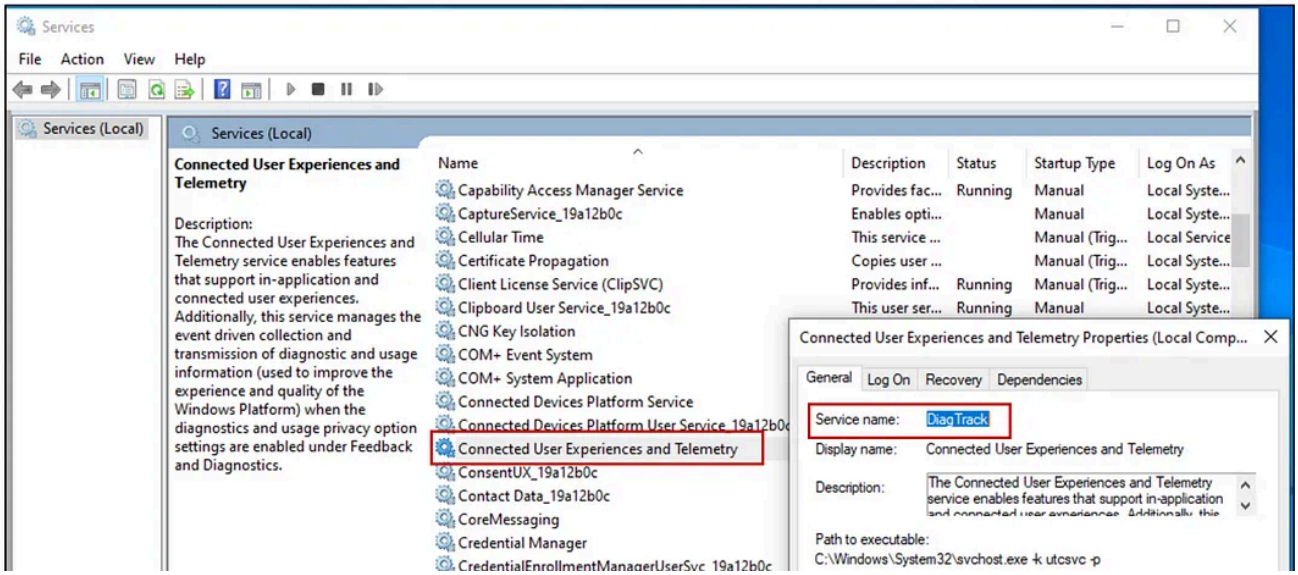


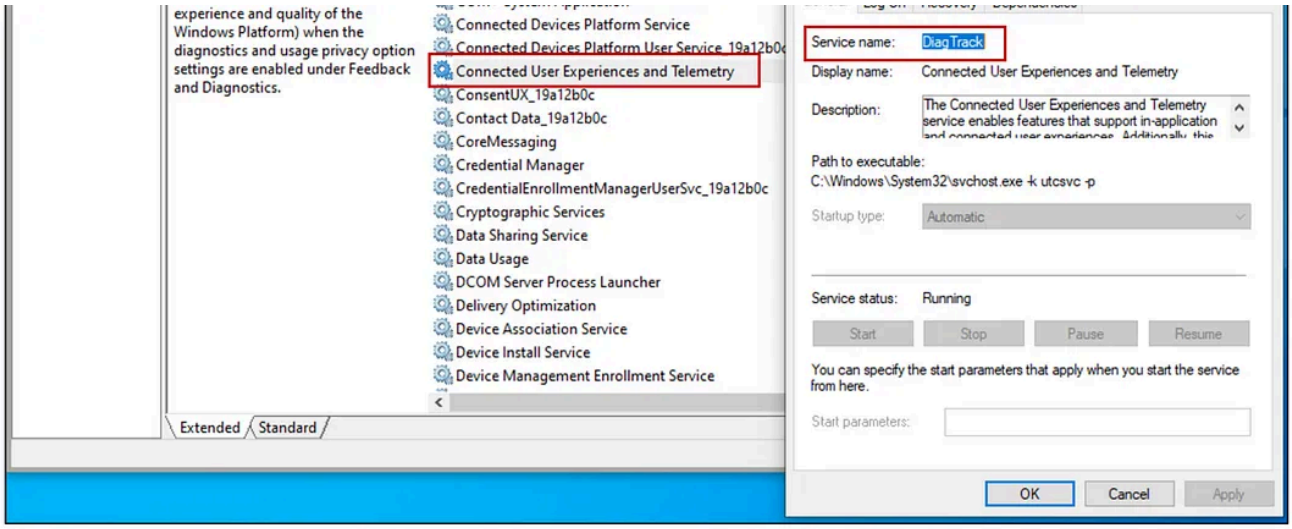

### Telemetry

Telemetry is a data collection system used by Microsoft to enhance the user experience by preemptively identifying security and functional issues in software. An application seamlessly shares data (crash logs, application-specific) with Microsoft to improve the user experience for future releases.

Telemetry functionality is achieved by Universal Telemetry Client (UTC) services available in Windows and runs through `diagtrack.dll`. Contents acquired through telemetry service are stored encrypted in a local folder `%ProgramData%\Microsoft\Diagnosis` and sent to Microsoft after 15 minutes or so.

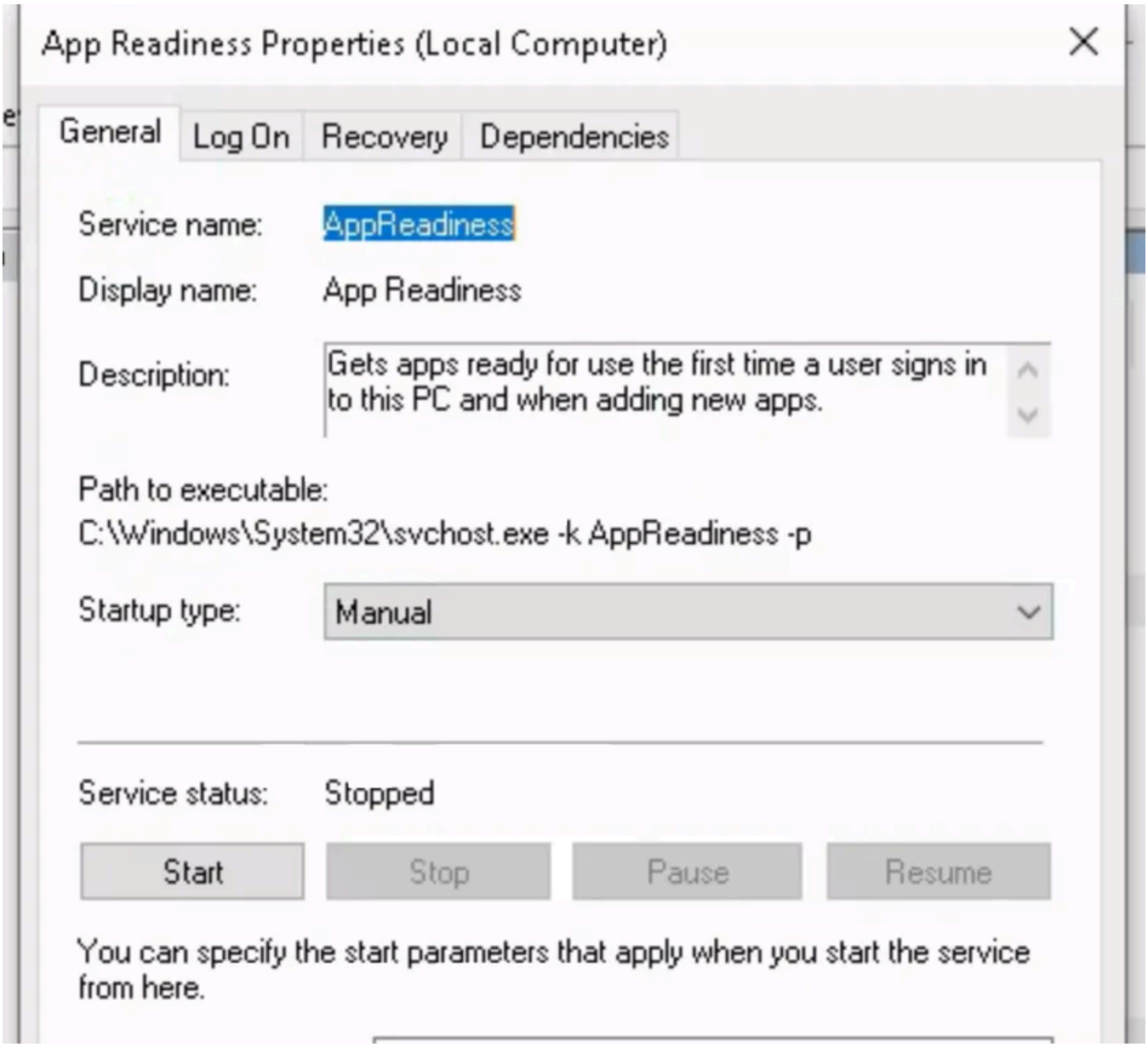
We can access `The DiagTrack` through the Services console in Windows 10.





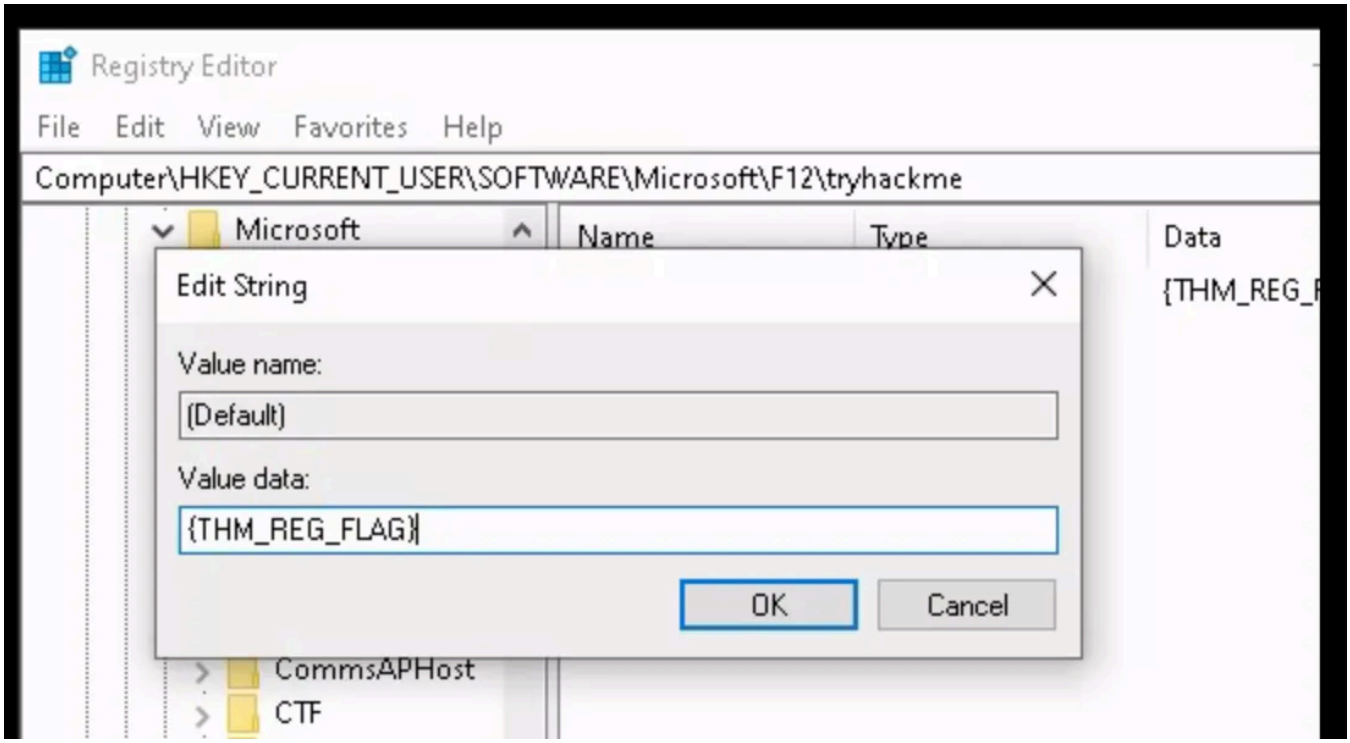

In subsequent tasks, we will harden Windows 10 through various techniques at the **User, Network, Application & Storage levels.**

What is the startup type of App Readiness service in the services panel?



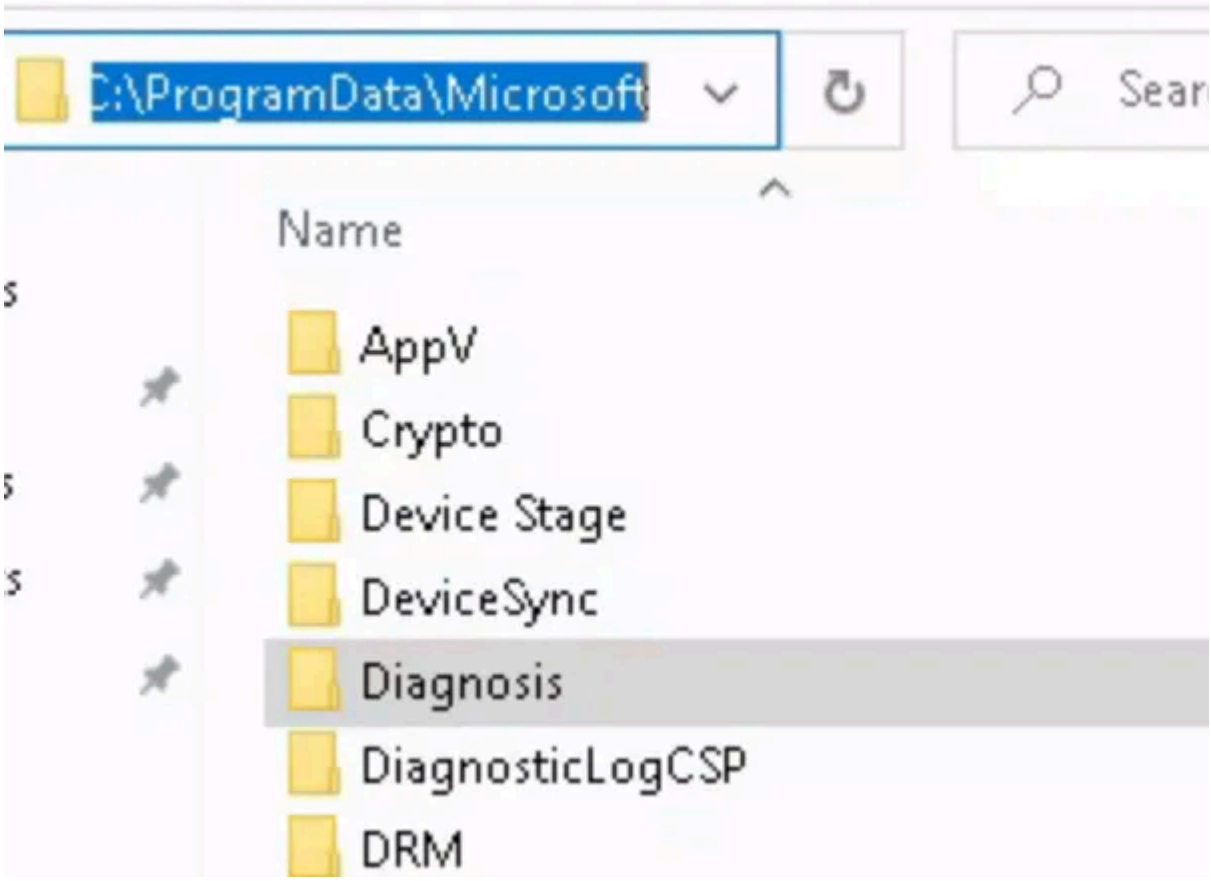

Answer: **Manual**

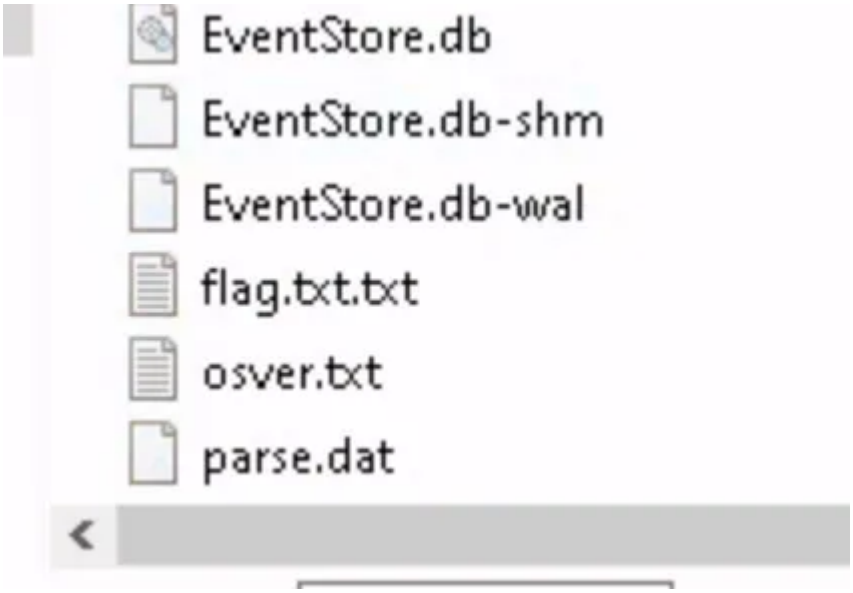
Open Registry Editor and find the key “tryhackme”. What is the default value of the key?

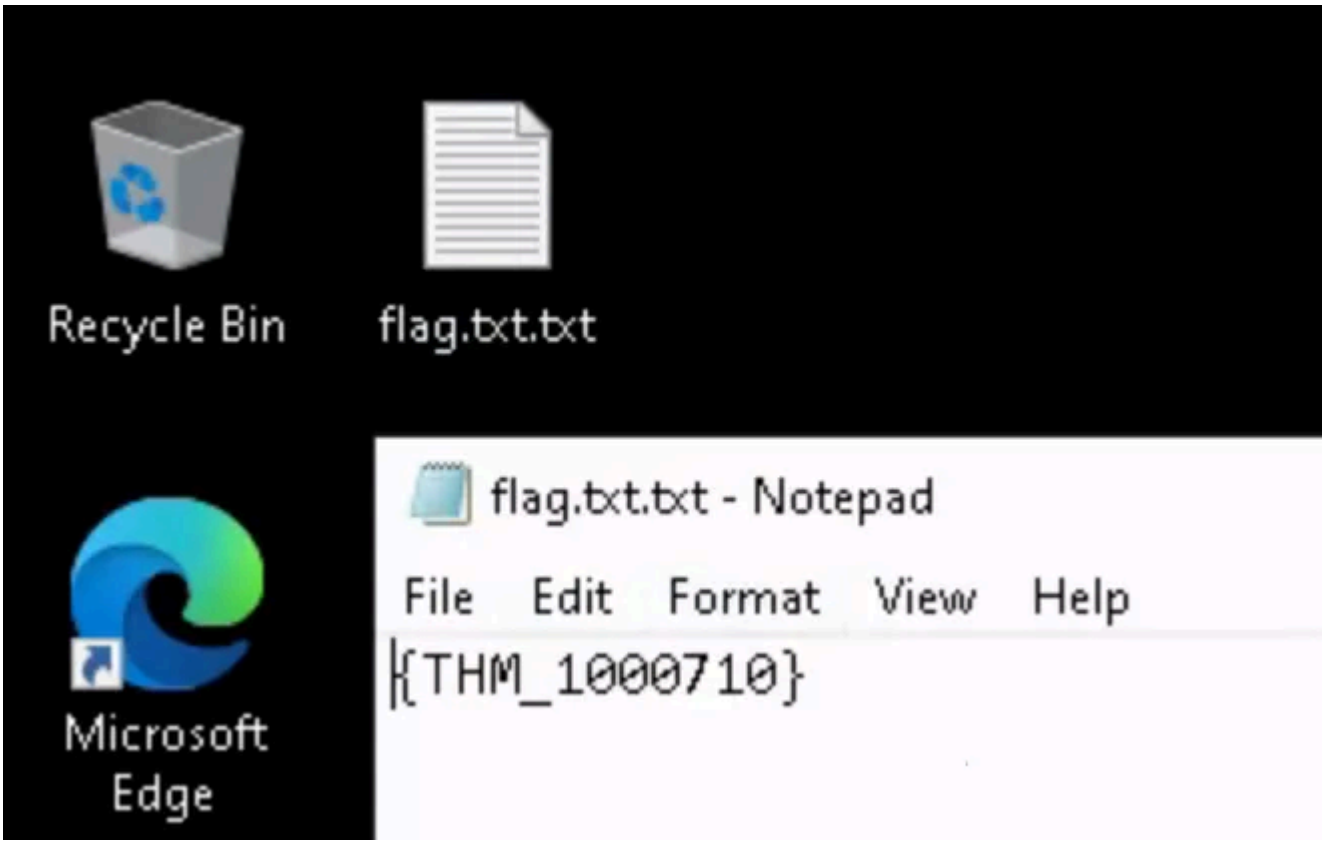



Answer: **{THM_REG_FLAG}**

Answer: Open the Diagnosis folder and go through the various log files. Can you find the flag?

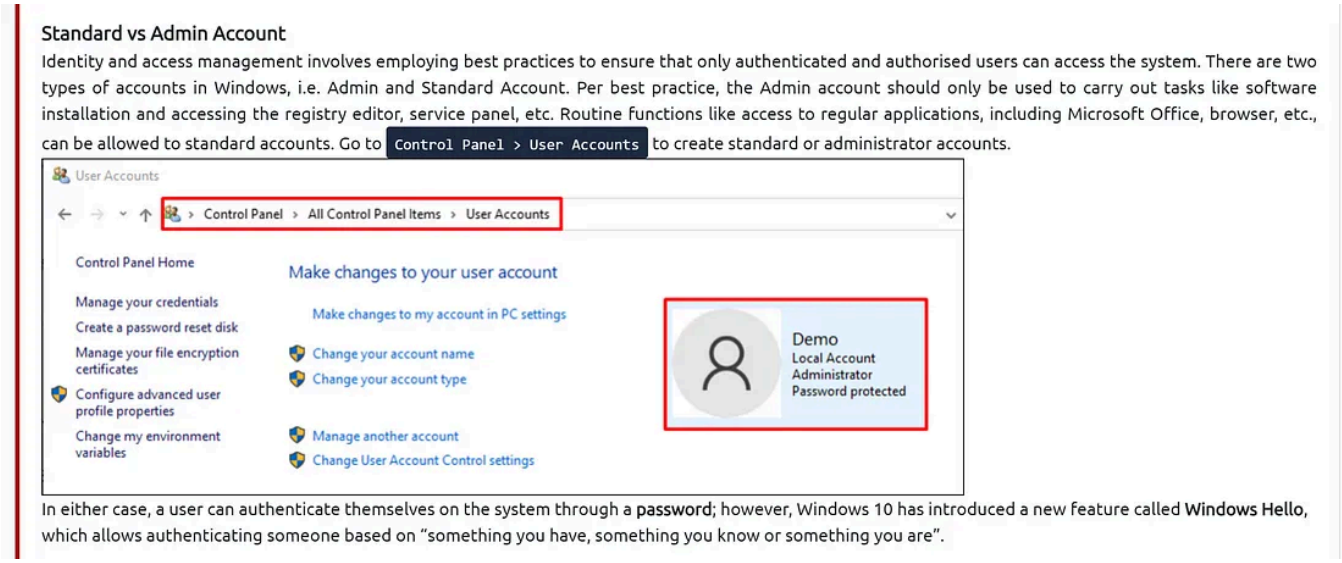

C:\ProgramData\Microsoft
Sear
Name
AppV
Crypto
Device Stage
DeviceSync
Diagnosis
DiagnosticLogCSP
DRM


EventStore.db
EventStore.db-shm
EventStore.db-wal
flag.txt.txt
osver.txt
parse.dat

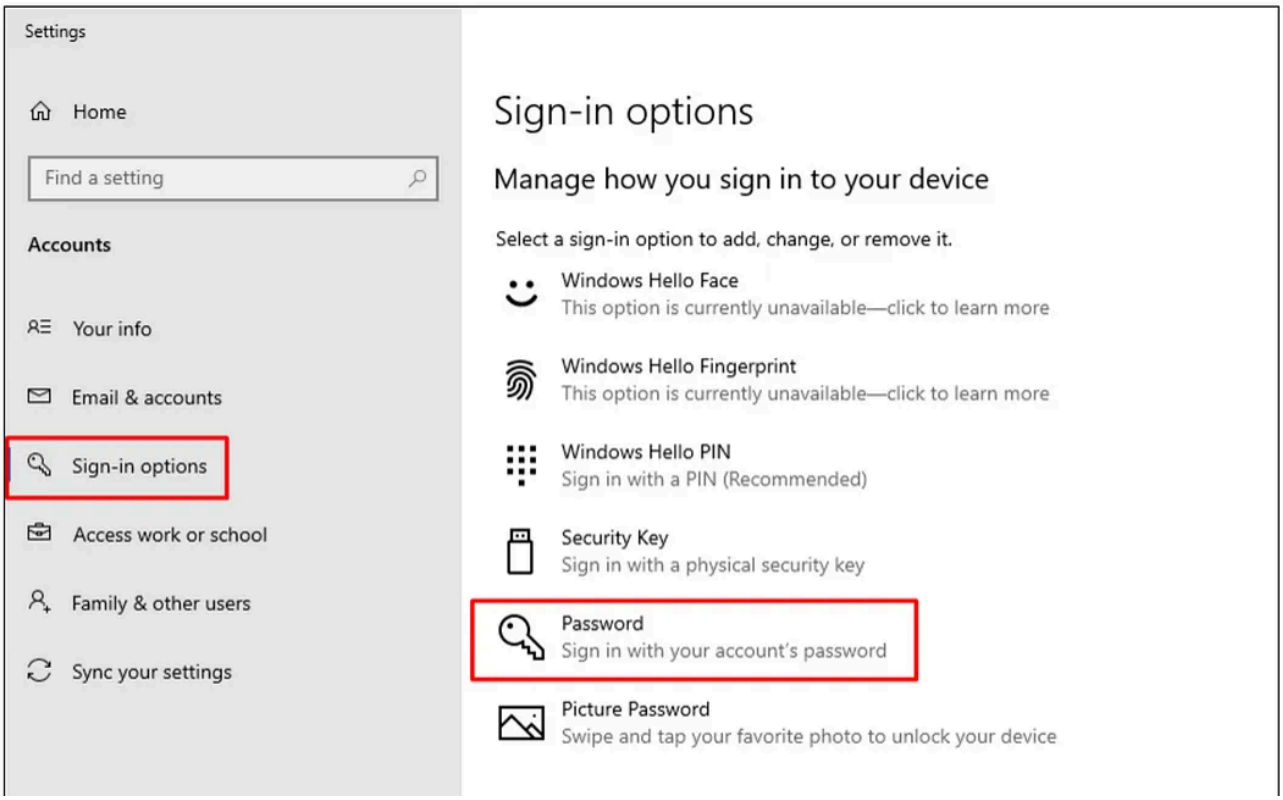



Answer: **{THM_1000710}**

## Task 3: **Identity & Access Management**



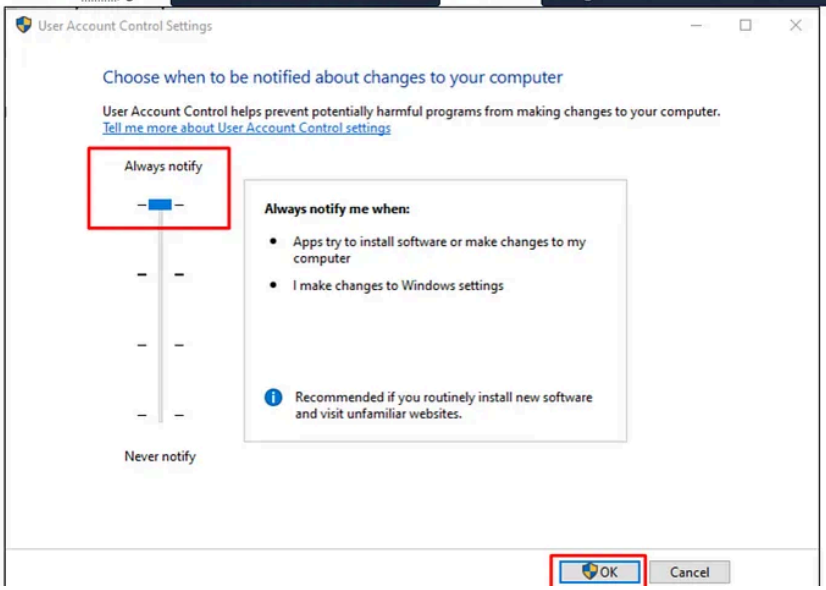
To access accounts and select the sign-in option, go to `Settings > Accounts > Sign-in Options.`




### User Account Control (UAC)

User Account Control (UAC) is a feature that enforces enhanced access control and ensures that all services and applications execute in non-administrator accounts. It helps mitigate malware's impact and minimises privilege escalation by bypassing UAC. Actions requiring elevated privileges will automatically prompt for administrative user account credentials if the logged-in user does not already possess these.
For example, installing device drivers or allowing inbound connections through Windows Firewall requires more permissions than already available privileges for a standard user. We have covered the topic in detail in Windows Fundamental 1.

As a principle, always follow the **Principle of Least Privilege**, which states that (Per CISA) "*a subject should be given only those privileges needed for it to complete its task. If a subject does not need an access right, the subject should not have that right*".
To access UAC, go to `Control Panel -> User Accounts` and click on `Change User Account Control Setting`.

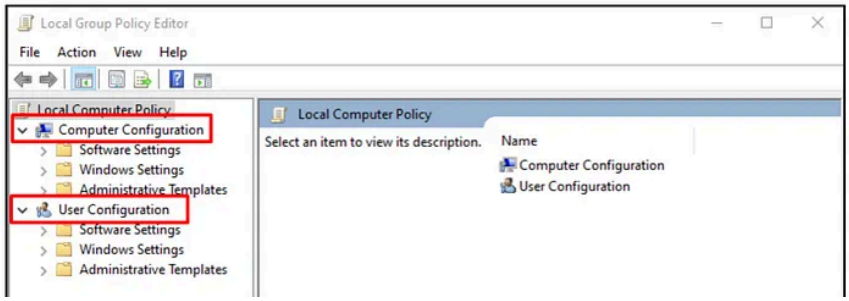


Keep the notification level "**Always Notify**" in the User Account Control Settings.

### Local Policy and Group Policies Editor

Group Policy Editor is a built-in interactive tool by Microsoft that allows to configure and implement local and group policies. We mainly use this feature when part of a network; however, we can also use it for a workstation to limit the execution of vulnerable extensions, set password policies, and other administrative settings.

**Note**: The feature is not available in Windows Home but only in the Pro and Enterprise versions.



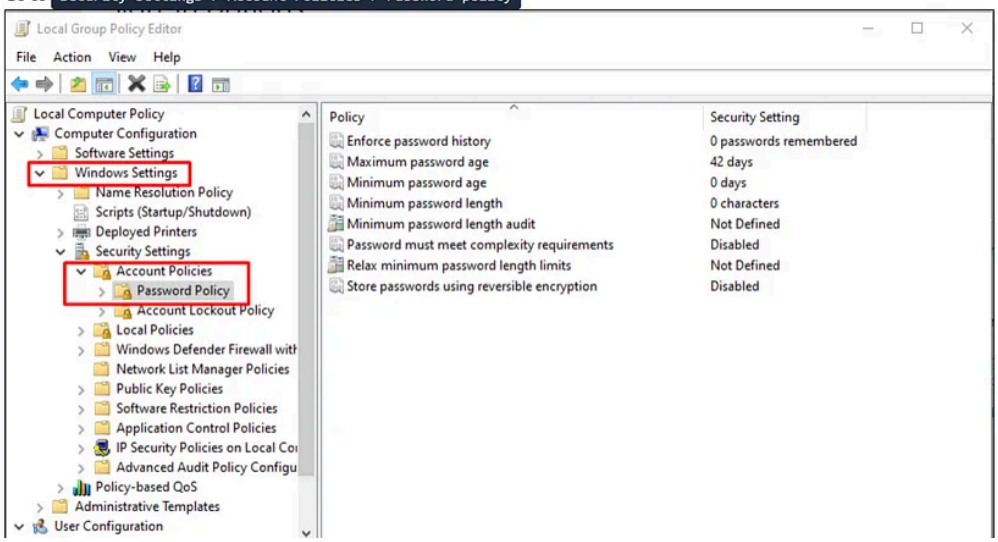

### Password Policies

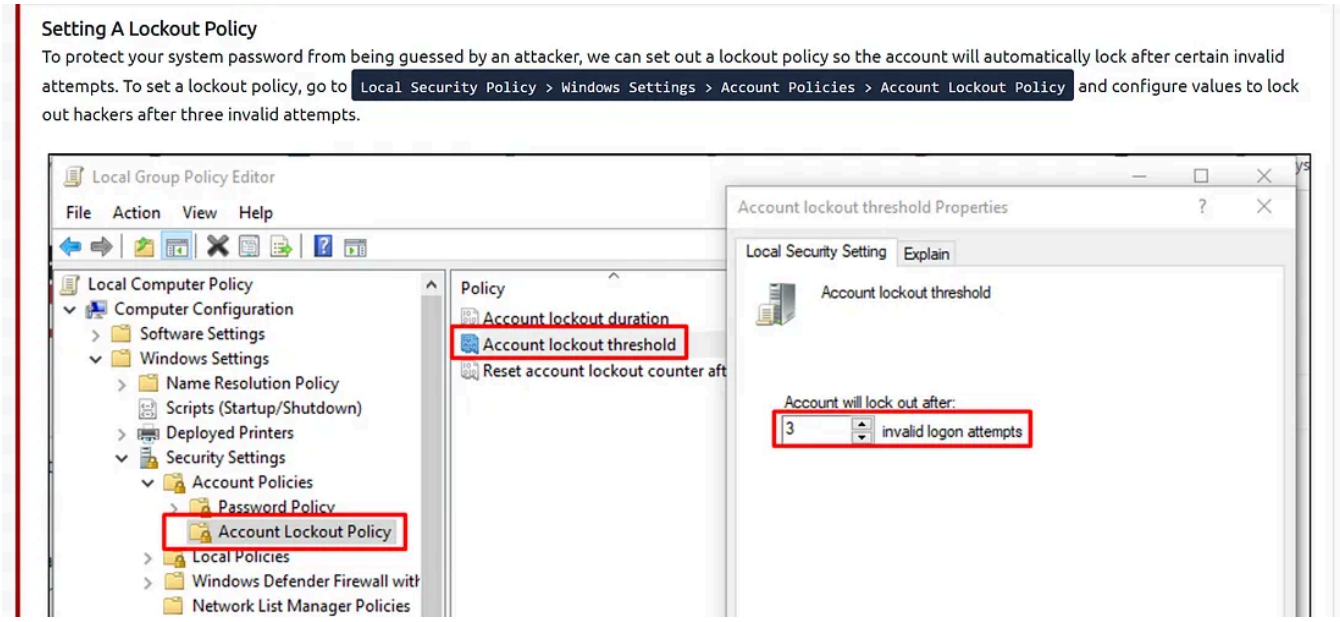
One primary use of a local policy editor is to ensure complex and strong passwords for user accounts. For example, we can design password policies to maximise our security:

- Passwords must contain both uppercase and lowercase characters.
- Check passwords against leaked or already hacked databases or a dictionary of compromised passwords.
- In case of 6 failed login attempts within 15 minutes, the account will remain locked for at least 1 hour.

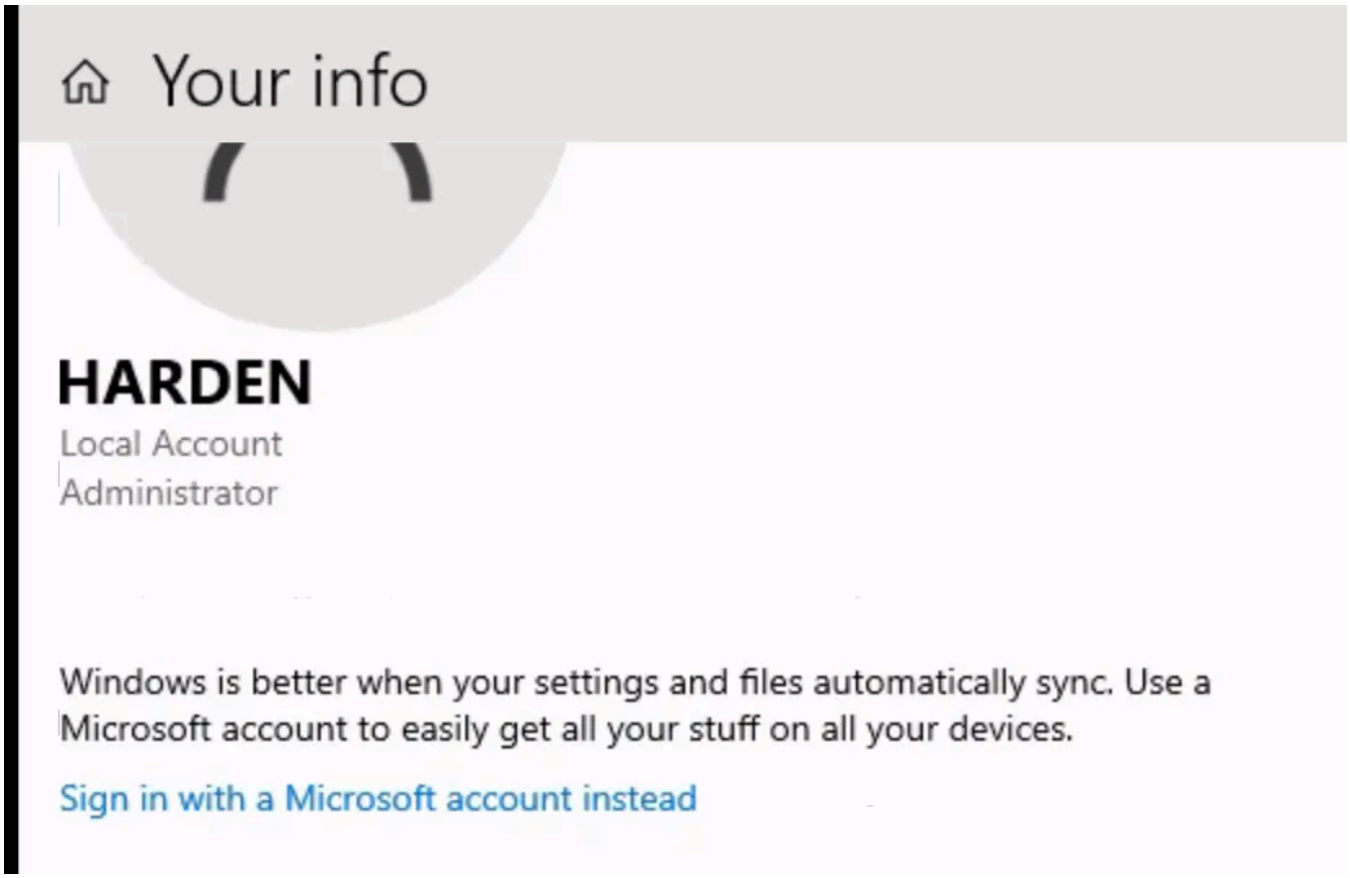
We can access Password policies through the Local group policy editor.

Go to `Security settings > Account Policies > Password policy`



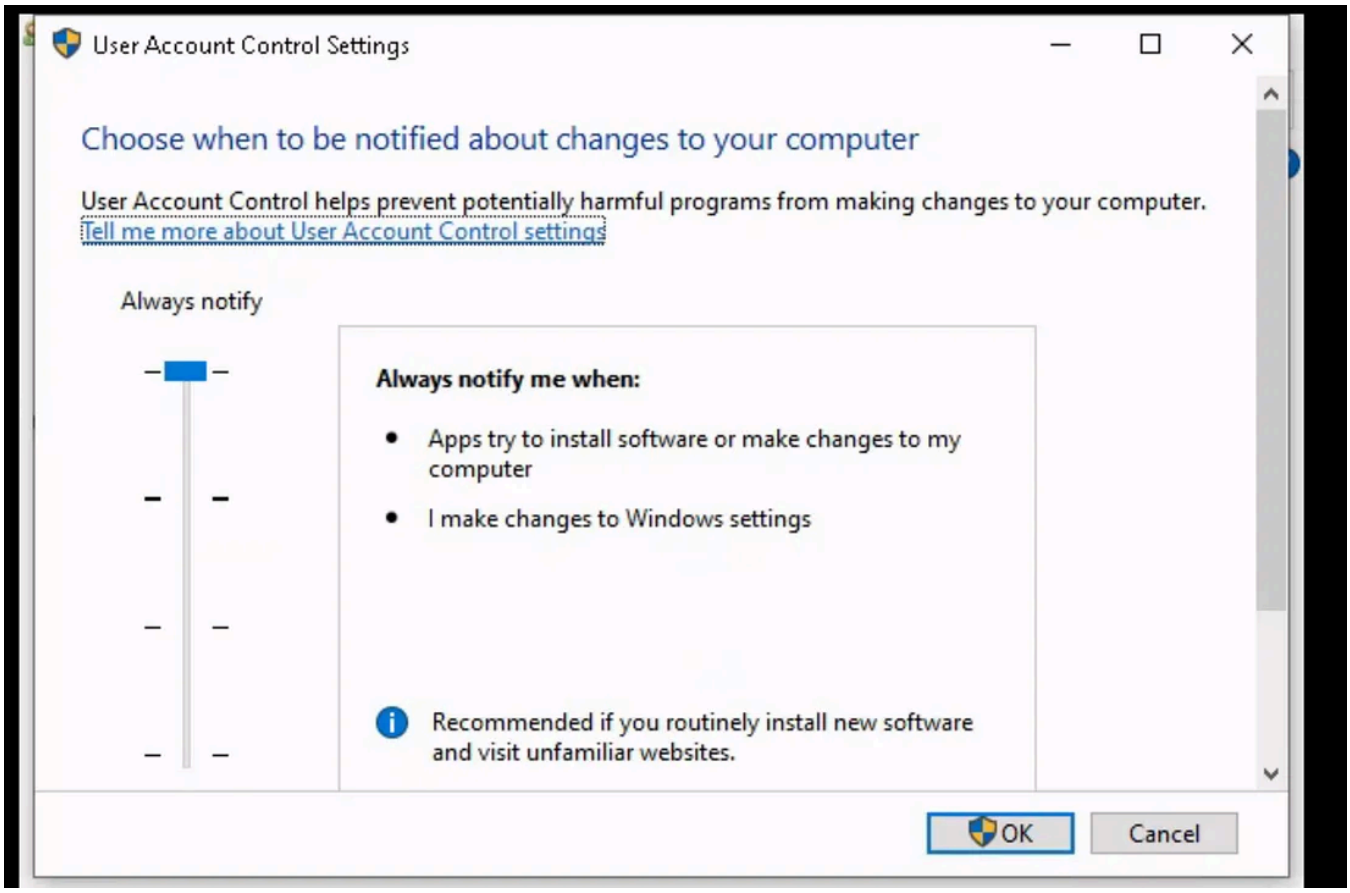



Find the name of the Administrator Account of the attached VM.



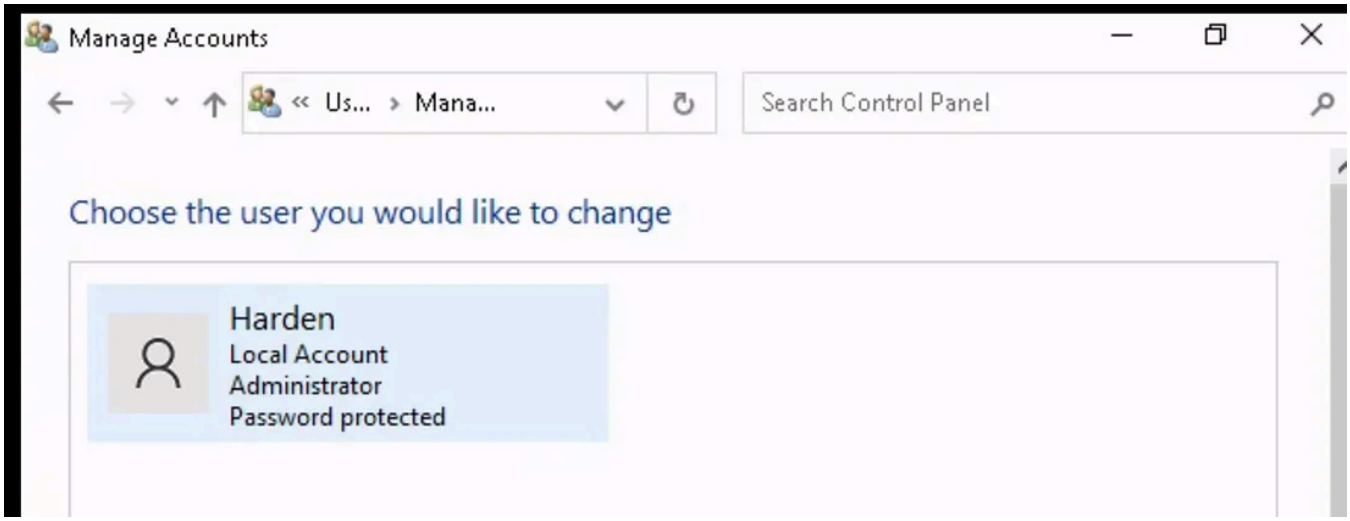

Answer: **Harden**

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




Answer: **Always Notify**

How many standard accounts are created in the VM?




Answer: **0**

Task 4: **Network Management**

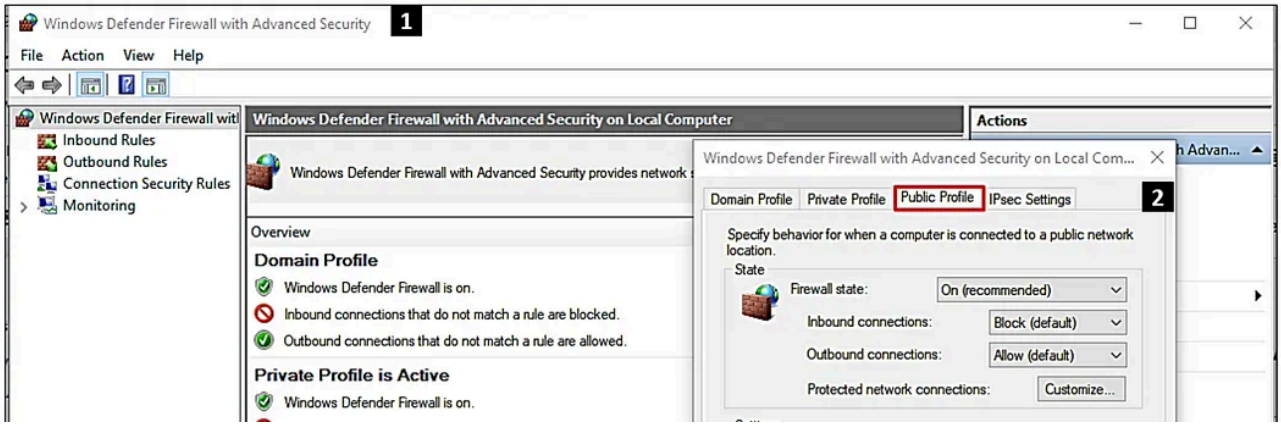
### Windows Defender Firewall

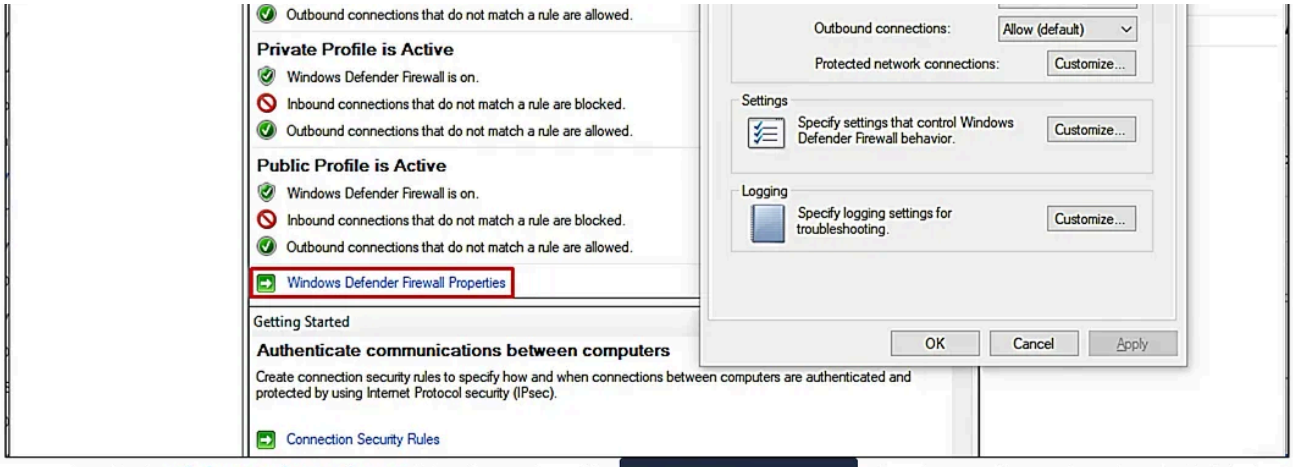
Windows Defender Firewall is a built-in application that protects computers from malicious attacks and blocks unauthorised traffic through inbound and outbound rules or filters. As an analogy, this is equivalent to "who is coming in and going out of your home".

Malicious actors abuse Windows Firewall by bypassing existing rules. For example, if we have configured the firewall to allow incoming connections, hackers will try to manipulate the functionality by creating a remote connection to the victim's computer.

You can see more details about Windows Firewall Configuration here.

We can access Windows Defender Firewall by accessing `WF.msc` in the Run dialogue.




As mentioned in the Windows Fundamentals room, it has three main profiles `Domain, Public and Private`. The Private profile must be activated with "Blocked Incoming Connections" while using the computer at home.

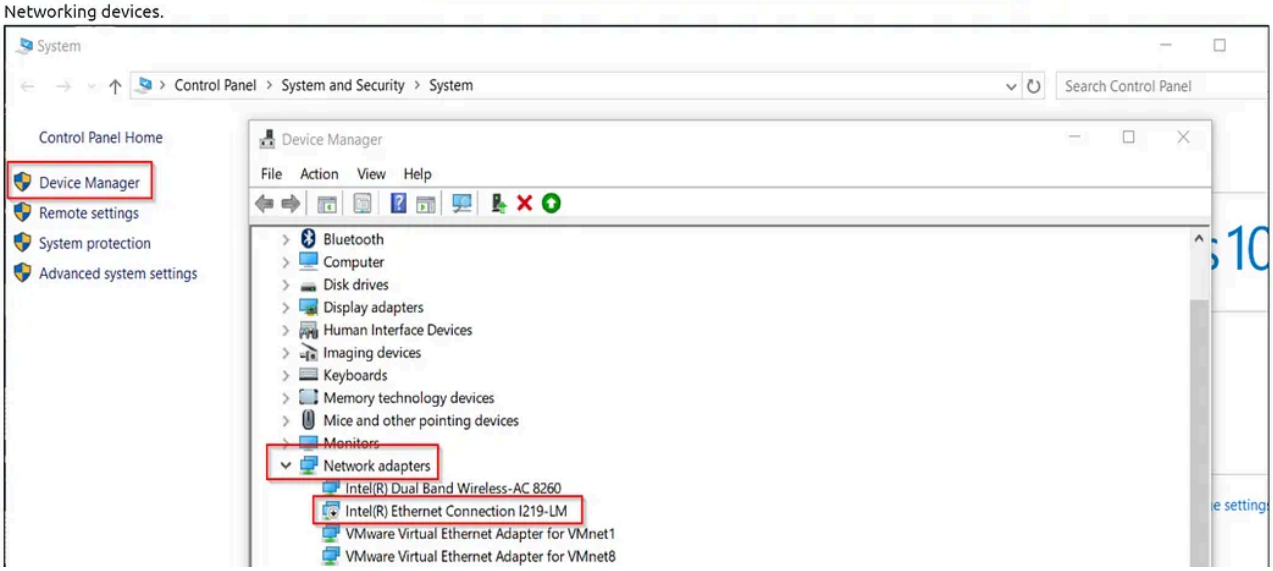
View detailed settings for each profile by clicking on Windows Defender Firewall Properties.

Whenever possible, enable the Windows Defender Firewall default settings. For blocking all the incoming traffic, always configure the firewall with a 'default deny' rule before making an exception rule that allows more specific traffic.

### Disable unused Networking Devices

Network devices like routers, ethernet cards, WiFI adapters etc., enable data sharing between computers. If the device is improperly configured or not being used by the owner, it is recommended to disable the interface so that threat actors cannot access them and use them for data retrieval from the victim's computer.

To disable the unused Networking Devices, go to the `Control panel > System and Security Setting > System > Device Manager` and disable all the unused Networking devices.




### Disable SMB protocol

SMB is a file-sharing protocol exploited by hackers in the wild. The protocol is primarily used for file sharing in a network; therefore, you must disable the protocol if your computer is not part of a network by issuing the following command in PowerShell.

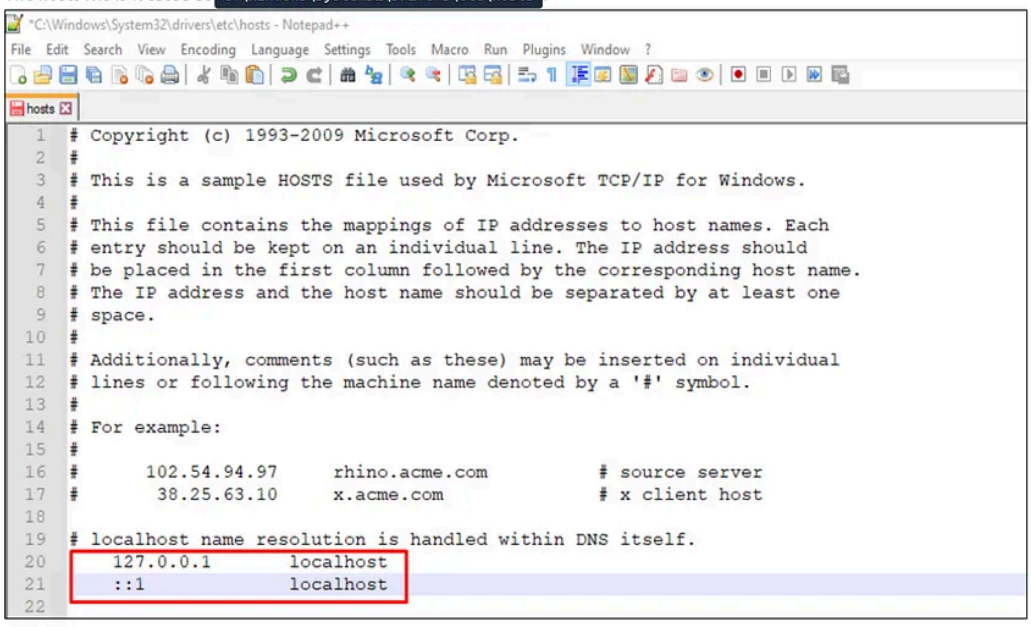
```
Administrator - Windows PowerShell

user@machine$ Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
Path          :
Online        : True
RestartNeeded : False
```

### Protecting Local Domain Name System (DNS)

The domain name system (DNS) is a naming system that translates Fully Qualified Domain Names (FQDN) into IP addresses. If the attacker places himself in the middle, he may intercept and manipulate DNS requests and point them to attacker-controlled systems since DNS replies are neither authenticated nor encrypted.

The hosts file located in Windows acts like local DNS and is responsible for resolving hostnames to IP addresses. Malicious actors try to edit the file's content to reroute traffic to their command and control server.

The hosts file is located at `C:\Windows\System32\Drivers\etc\hosts`.



### Mitigating Address Resolution Protocol Attack

The address resolution protocol resolves MAC addresses from given IP addresses saved in the workstations ARP cache. The ARP offers no authentication and accepts responses from any user in the network. An attacker can flood target systems with crafted ARP responses, which point to an attacker-controlled machine and put him in the middle of communication between the targeted hosts.

You can check ARP entries using the command `arp -a` in the command prompt.

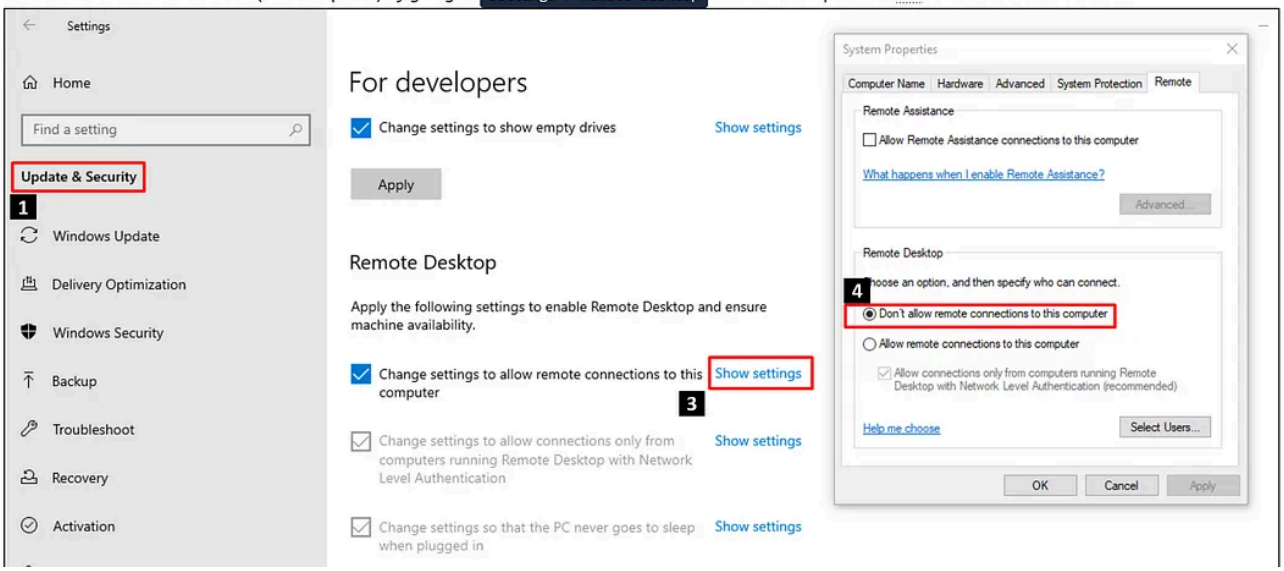

The table contains MAC addresses in the middle and IP addresses in the left. If the table includes a MAC mapped to two IPs, you are probably susceptible to an ARP poisoning attack.

To clear the ARP cache and prevent the attack, issue the command `arp -d`.

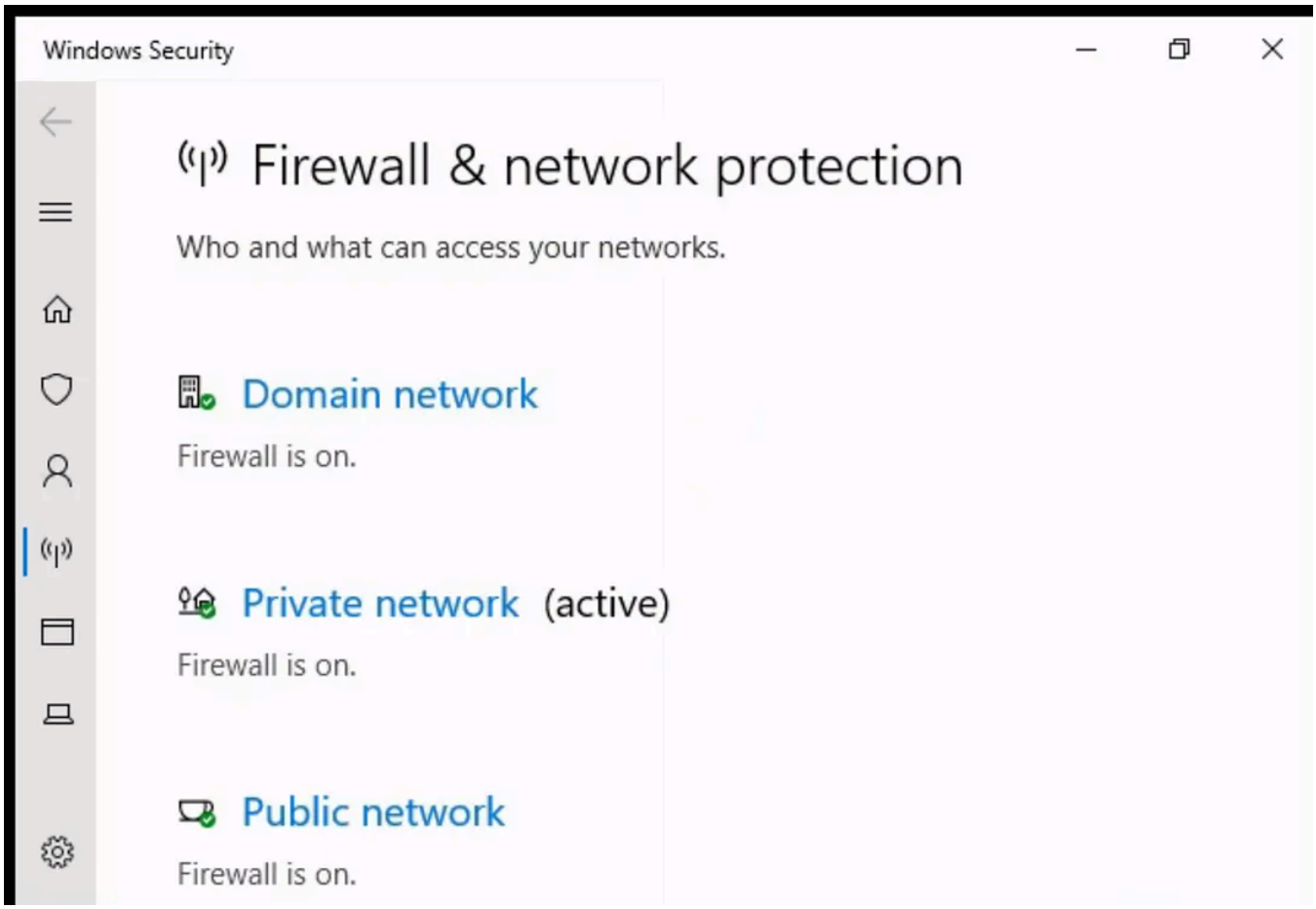
### Preventing Remote Access to Machine

Remote access provides a way to connect to other computers/networks even located at a different geographical location for file sharing and remotely make changes to a workstation. Microsoft has developed a Remote Desktop Protocol (RDP) for connecting with other computers. Hackers have exploited the protocol in the past, like the famous Blue Keep vulnerability, to gain unauthorised access to the target system.

We must disable remote access (if not required) by going to `settings > Remote Desktop`. Do not attempt this in VM attached to this room.

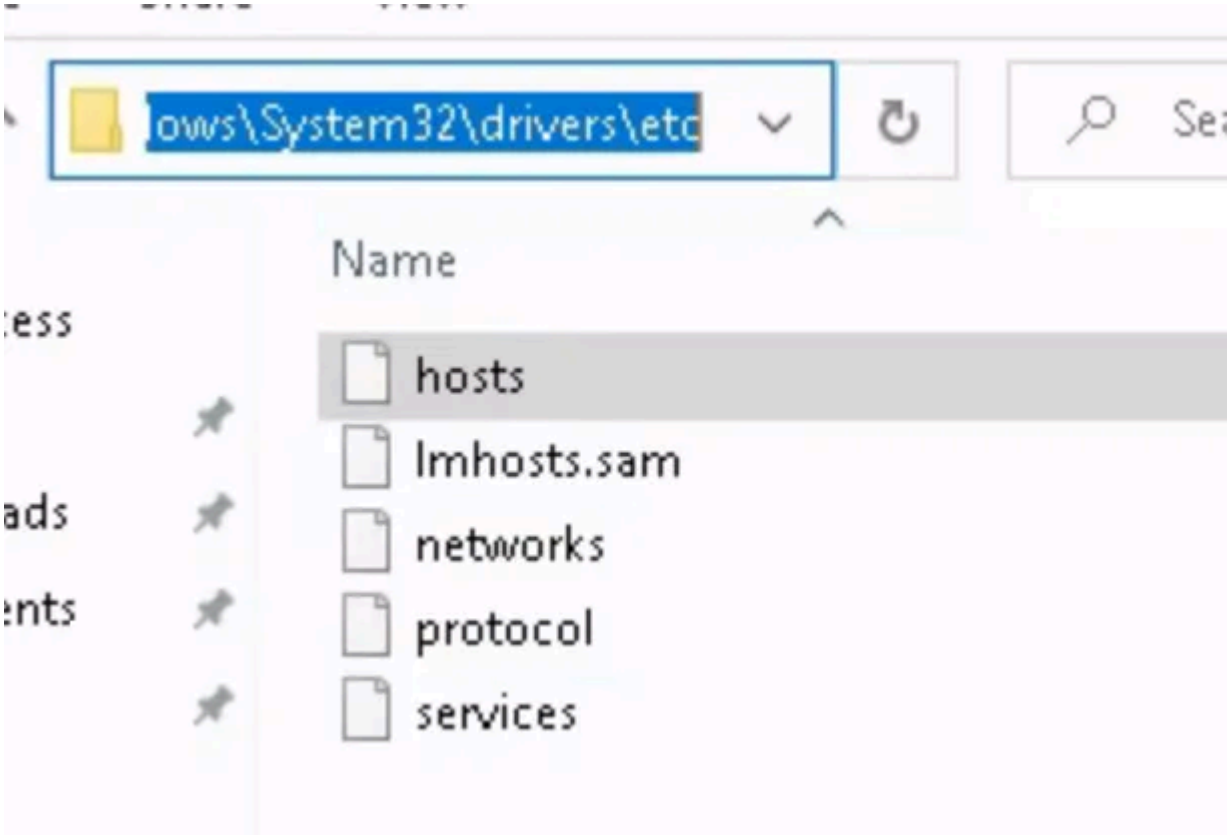


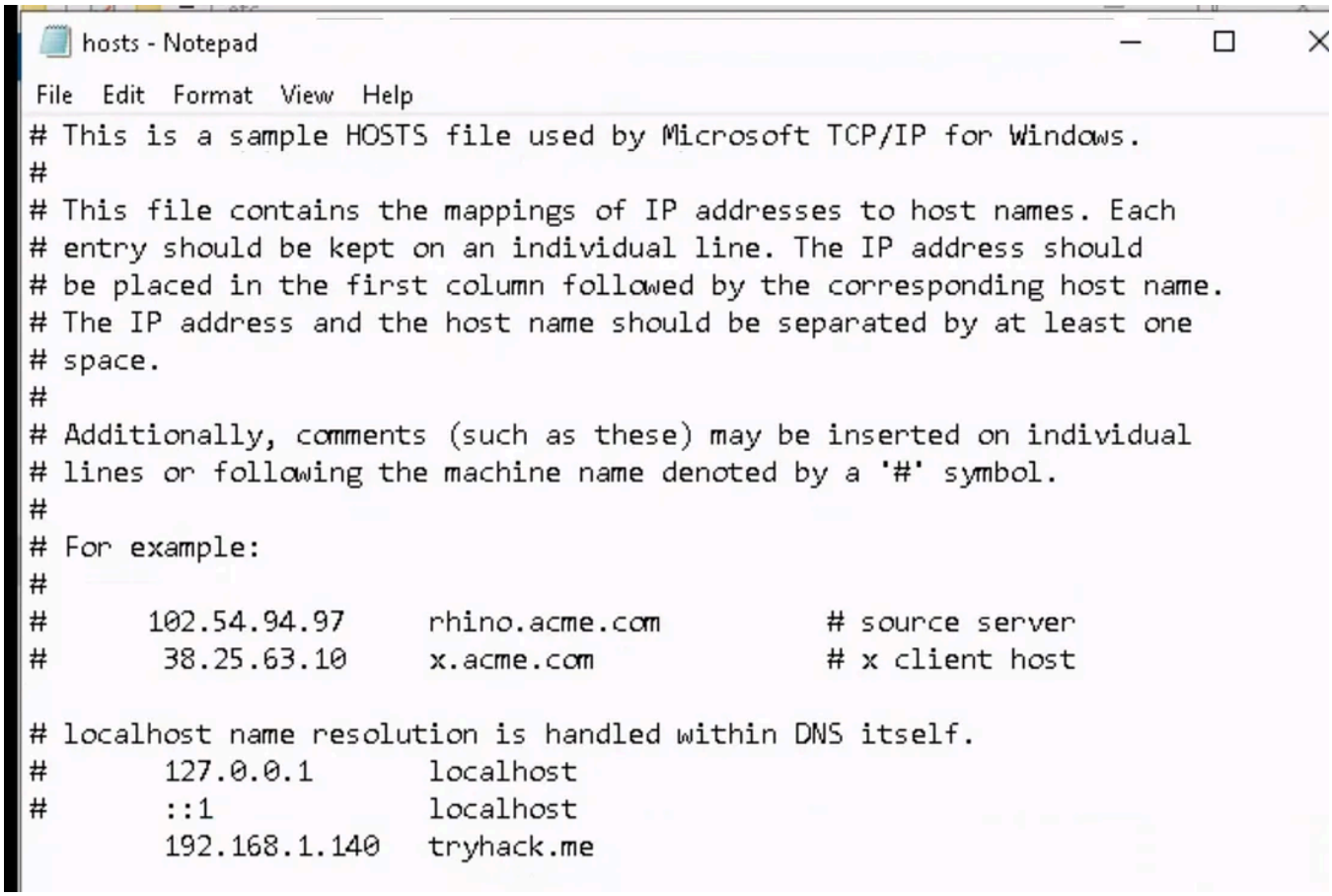

Open Windows Firewall and click on Monitoring in the left pane — which of the following profiles is active? Domain, Private, Public?




Answer: **Private**

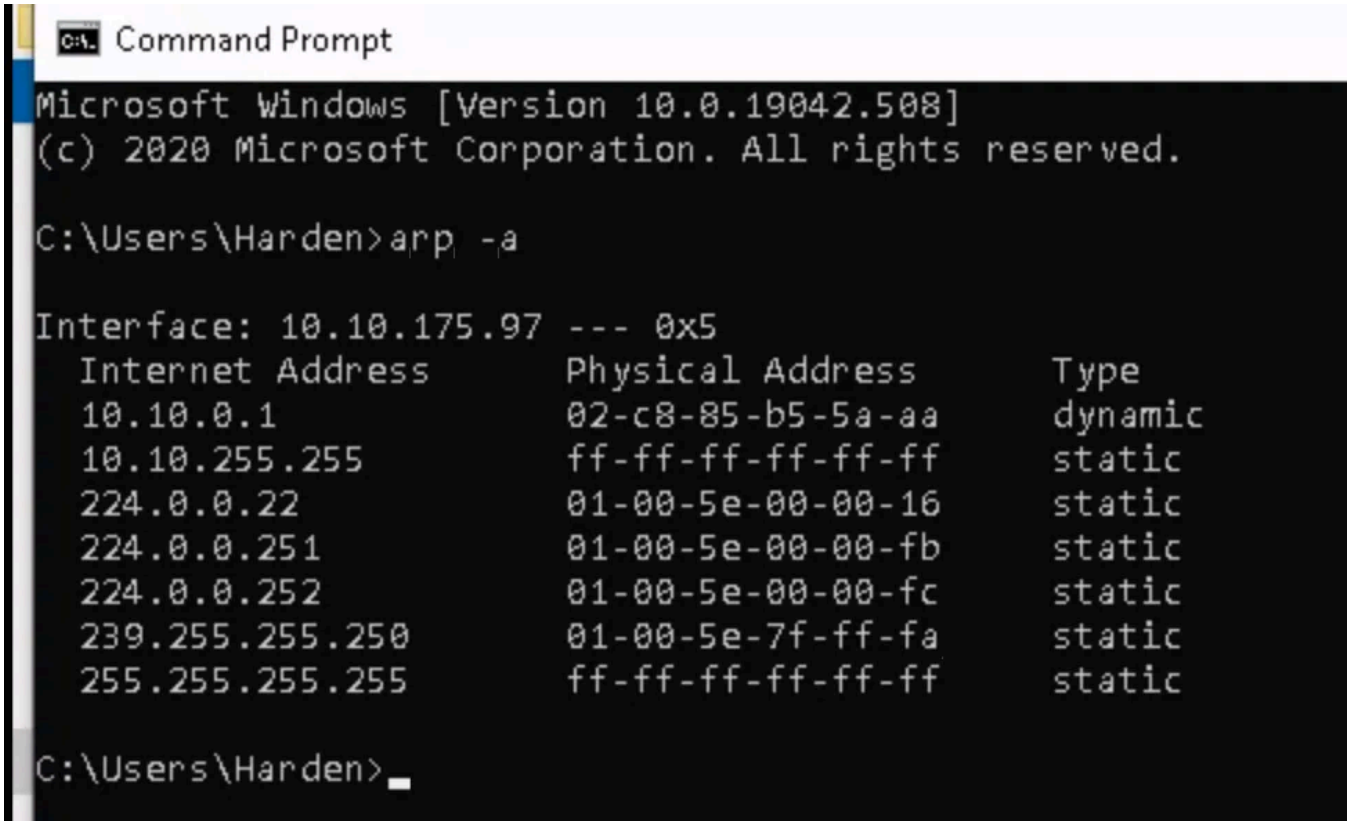
Find the IP address resolved for the website tryhack.me in the Virtual Machine as per the local hosts file.






Answer: **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?



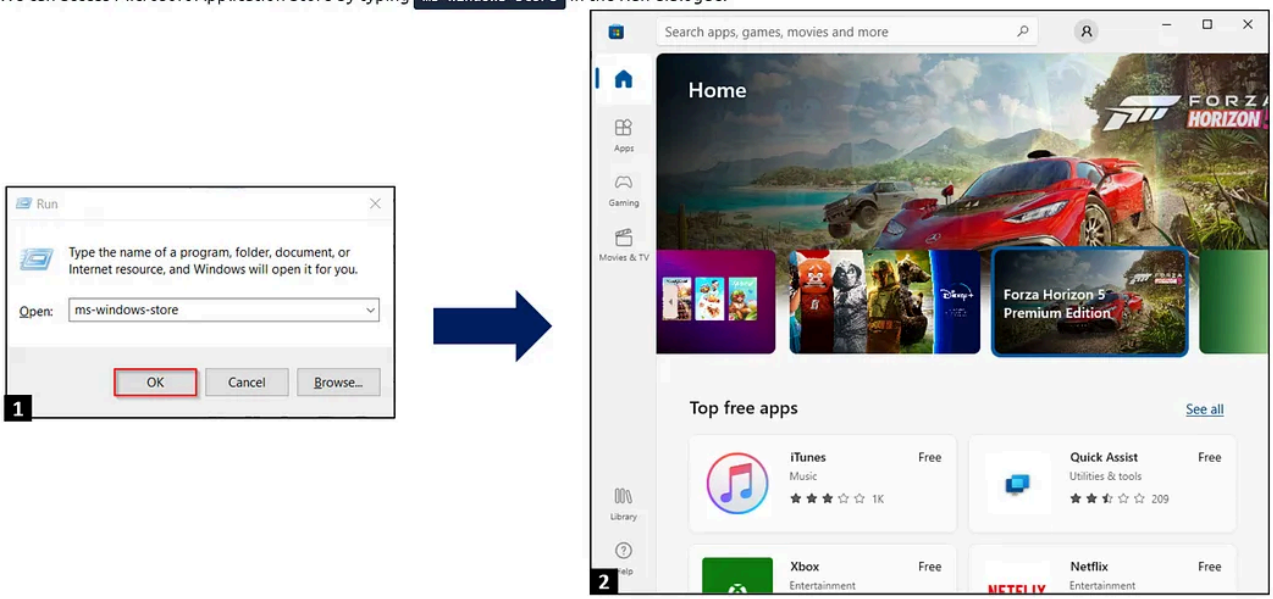
Answer: **ff-ff-ff-ff-ff-ff**

## Task 5: **Application Management**

**Trusted Application Store**

Microsoft Store offers a complete range of applications (games, utilities) and allows downloading non-malicious files through a single click. Malicious actors bind legitimate software with trojans and viruses and upload it on the internet to infect and access the victim's computer. Therefore, downloading applications from the Microsoft Store ensures that the downloaded software is not malicious.

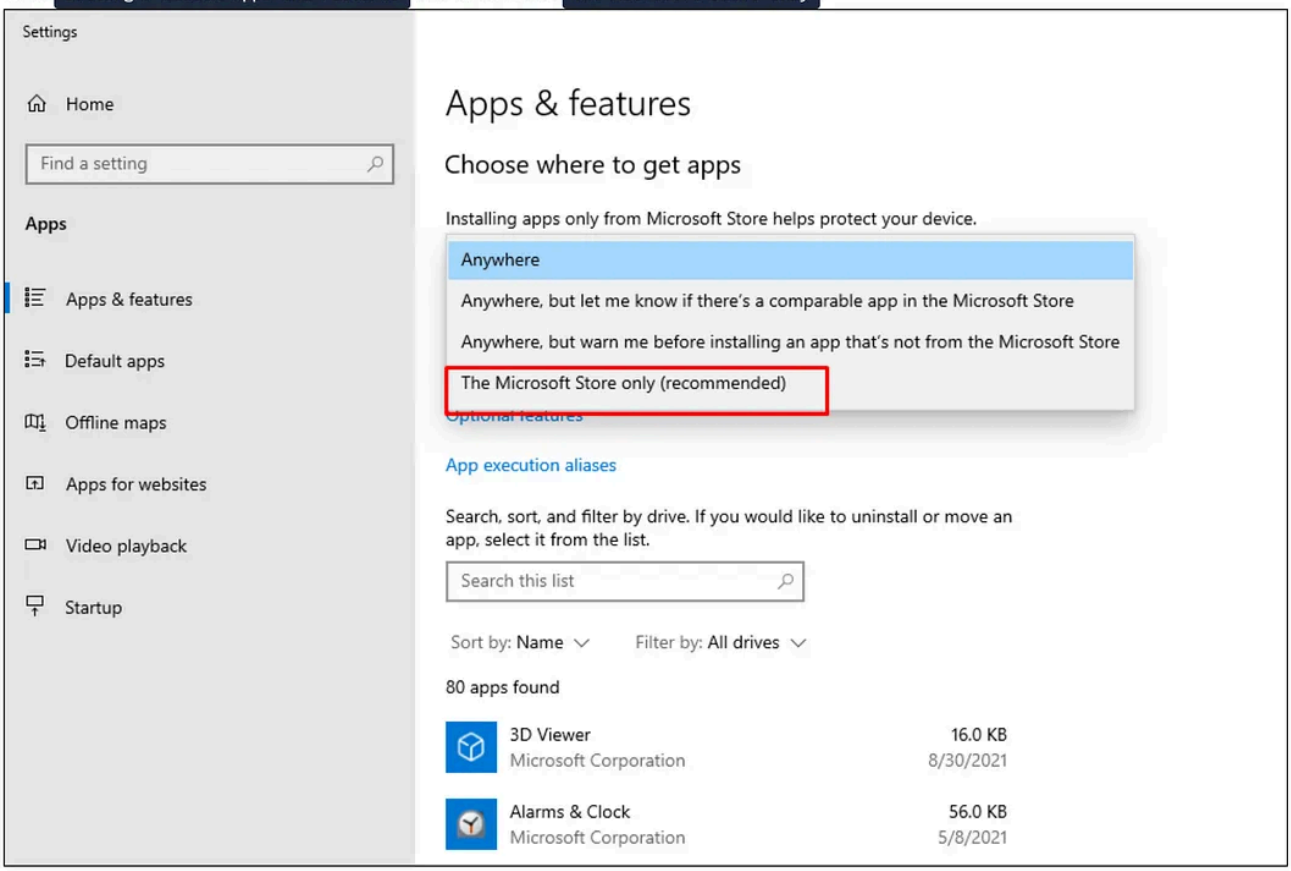
We can access Microsoft Application Store by typing `ms-windows-store` in the Run dialogue.




**Safe App Installation**

Only allow installation of applications from the Microsoft Store on your computer.

Go to `Setting > Select Apps and Features` and then select `The Microsoft Store only`.



### Malware Removal through Windows Defender Anti Virus

Windows Defender Anti Virus is a complete anti-malware program capable of identifying malicious programs and taking remedial measures like quarantine. The program used to have an entire Graphical User Interface; however, Windows 10 and newer versions manage the same through Windows Security Centre. Windows Defender primarily offers four main functionalities:

- **Real-time protection** - Enables periodic scanning of the computer.
- **Browser integration** - Enables safe browsing by scanning all downloaded files, etc.
- **Application Guard** - Allows complete web session sandboxing to block malicious websites or sessions to make changes in the computer.
- **Controlled Folder Access** - Protect memory areas and folders from unwanted applications.

You have already learned about this in Windows Fundamentals 3

### Microsoft Office Hardening

Microsoft Office Suite is one of the most widely used application suites in all sectors, including financial, telecom, education, etc. Malicious actors abuse its functionality through macros, Flash applets, object linking etc., to achieve Remote Code Execution.

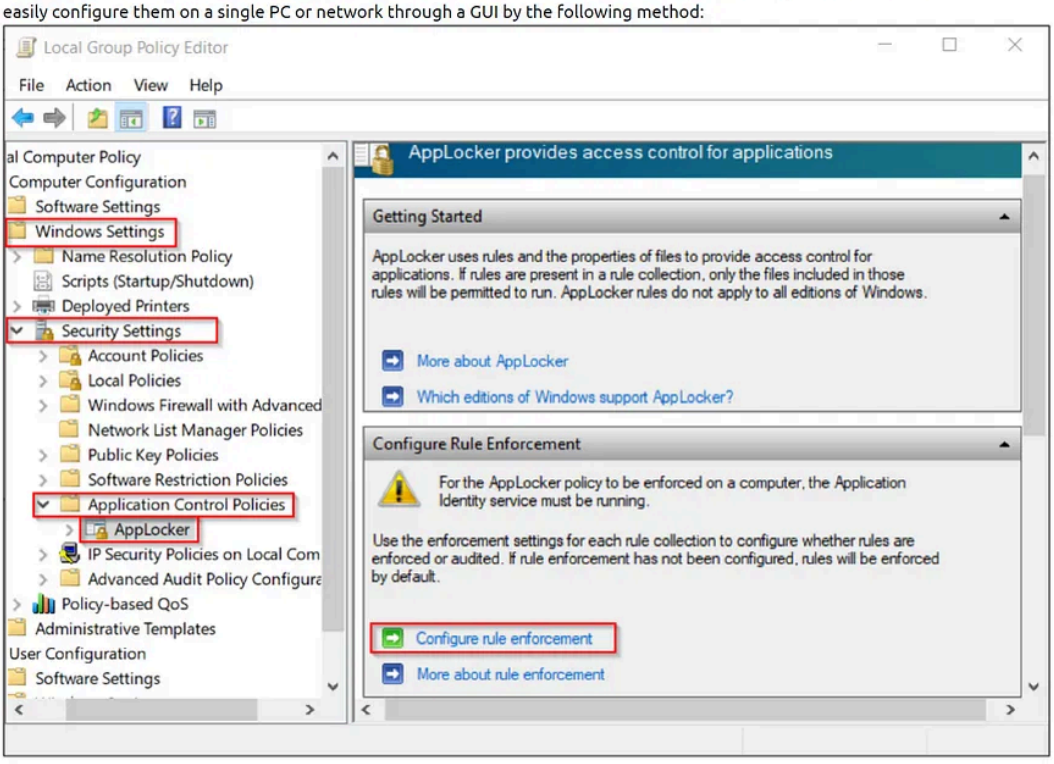
Hardening of Microsoft Office may vary from person to person as legitimate functionality of Microsoft Office is exploited to gain access. For example, disabling macros in a University may be helpful as no one uses it; however, banks cannot disable macros as they heavily rely on complex invoices and formulas through macros.

The attached VM contains a batch file based on best practices and Microsoft Attack Surface Reduction Rules for hardening Microsoft Office. To execute the script, right-click on the file `office.bat` on Desktop and Run as Administrator.

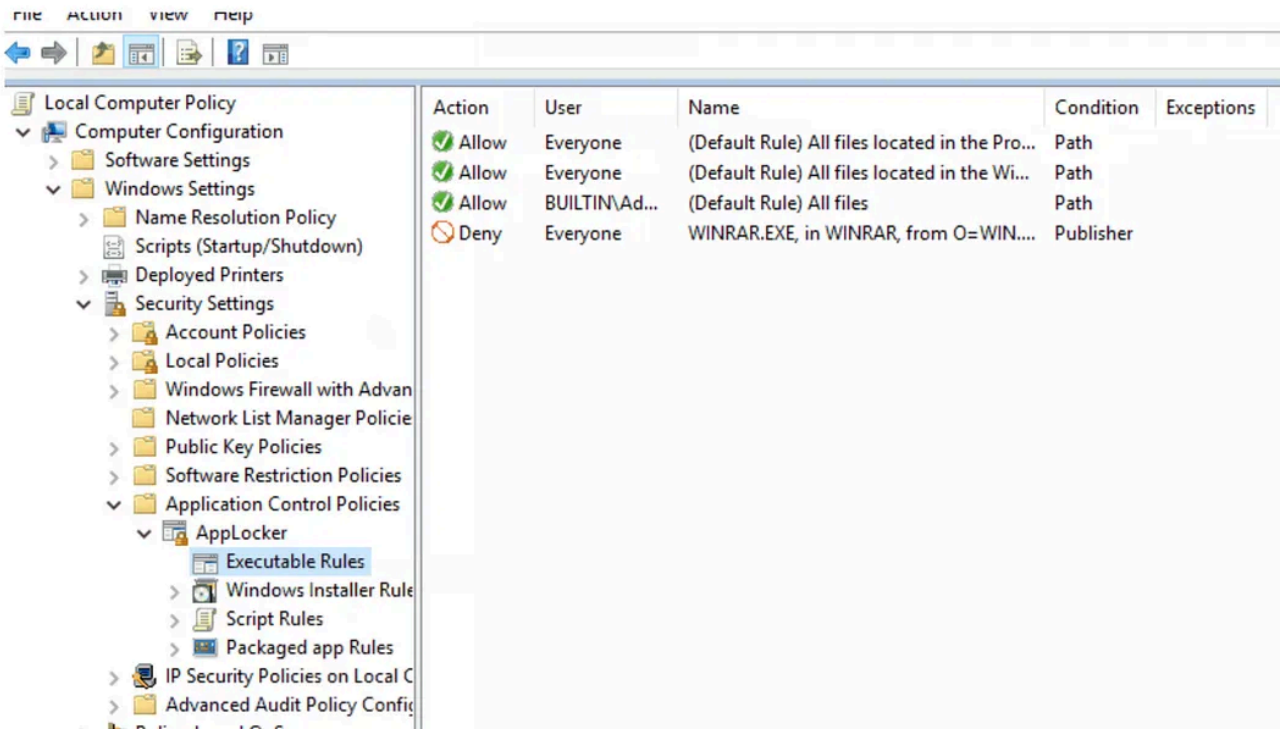
```
Command Prompt - Administrator

harden@tryhackme$ office.bat (Work in Progress)
Microsoft Office Hardened Successfully.
```

### AppLocker

AppLocker is a recently introduced feature that allows users to block specific executables, scripts, and installers from execution through a set of rules. We can easily configure them on a single PC or network through a GUI by the following method:



Now, we will see how to add a rule through AppLocker to block a file based on its publisher name.




### Browser (MS Edge)

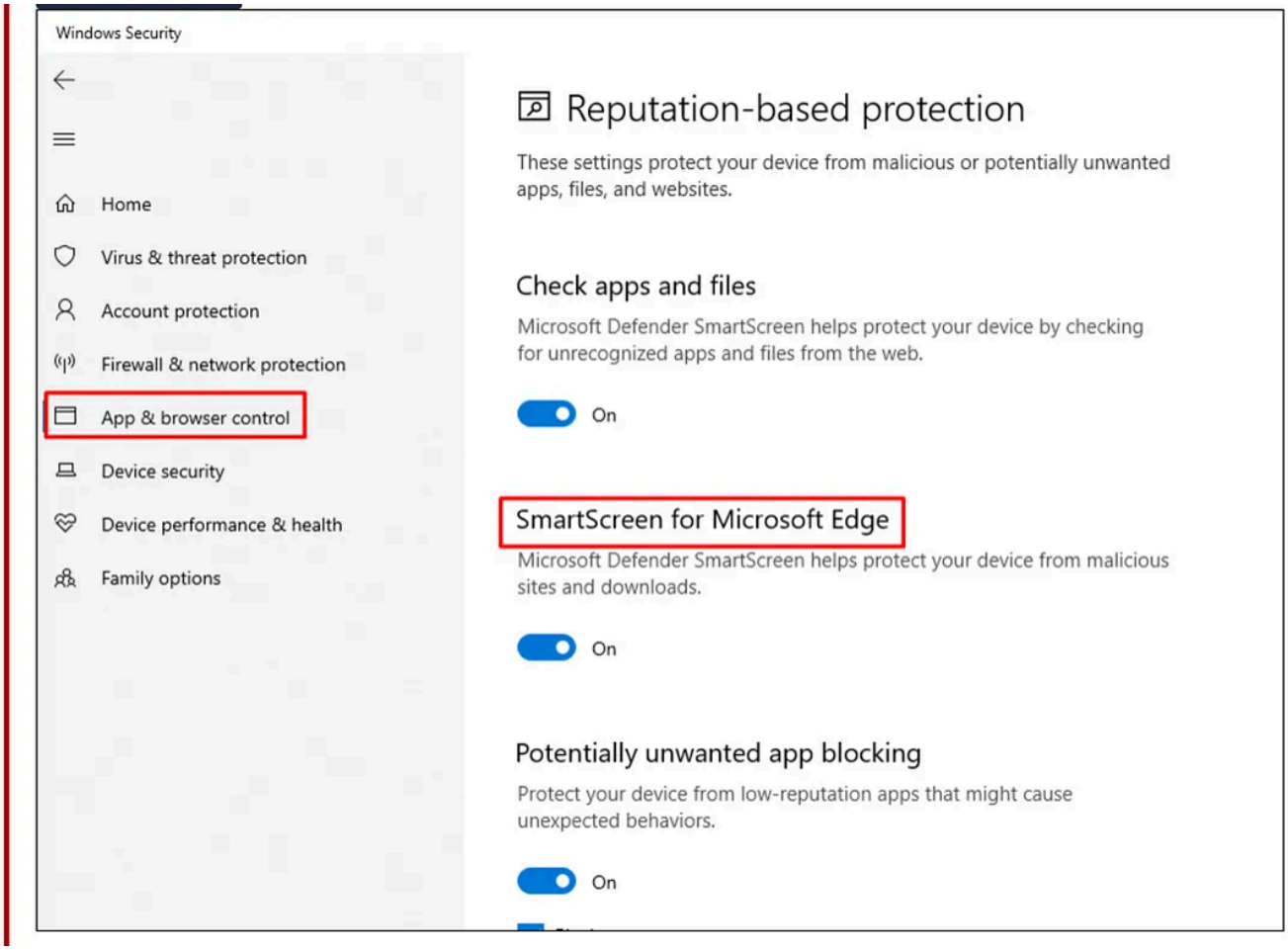
Microsoft Edge is a built-in browser available on Windows machines based on Chromium, inline with Google Chrome and Brave. The browser often acts as an entry point to a system for further pivoting and lateral movement. It is therefore of utmost importance to block and mitigate critical attacks carried out through a browser that include ransomware, ads, unsigned application downloads and trojans.

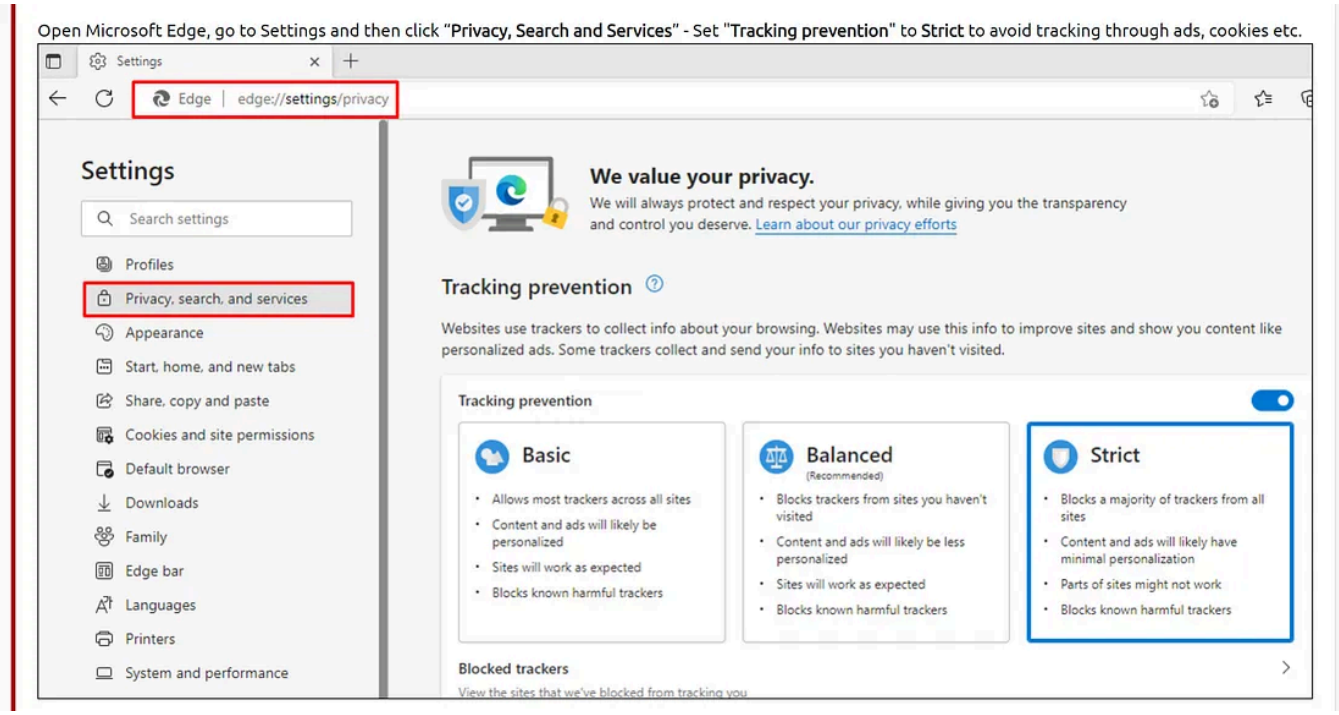
### Protecting the Browser through Microsoft Smart Screen

Microsoft SmartScreen helps to protect you from phishing/malware sites and software when using Microsoft Edge. It helps to make informed decisions for downloads and lets you browse safely in Microsoft Edge by:

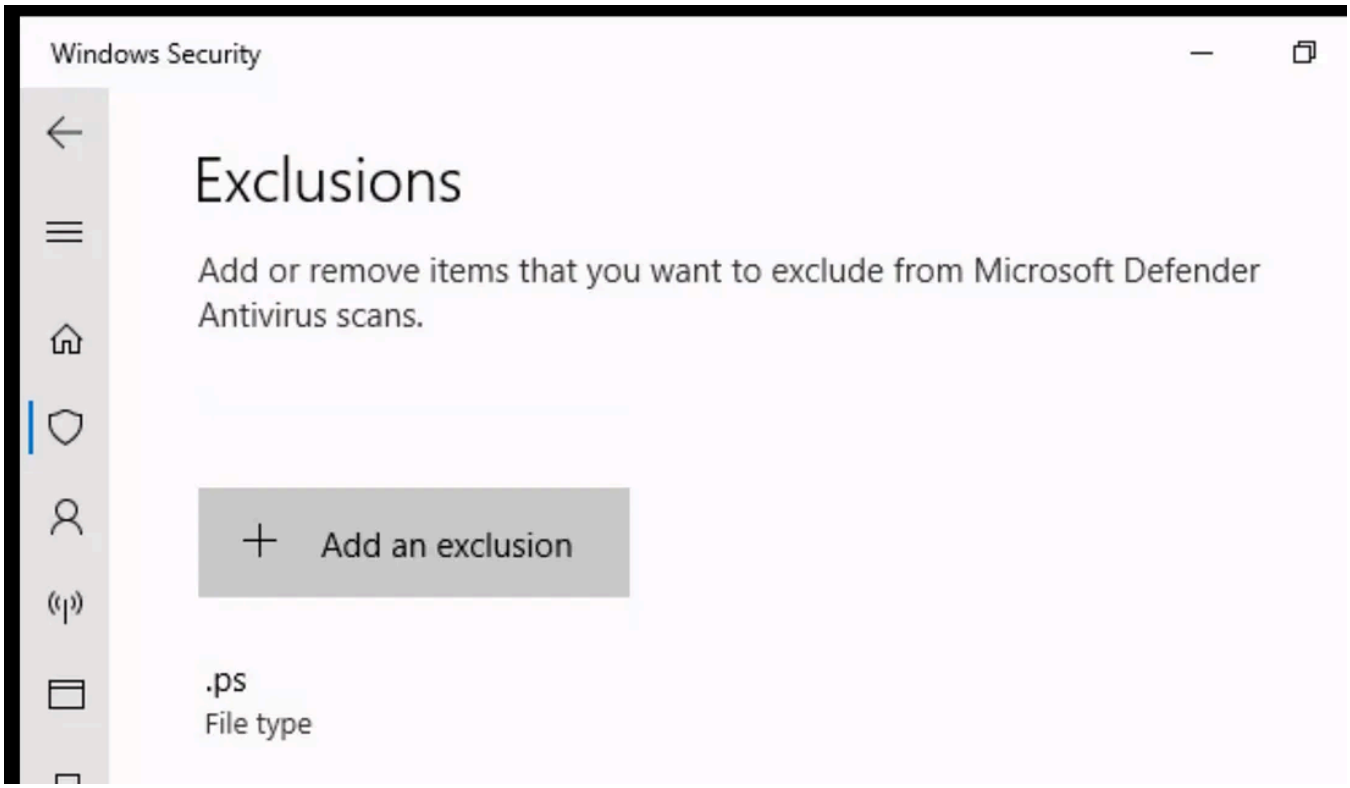
- Displaying an alert if you are visiting any suspicious web pages.
- Vetting downloads by checking their hash, signature etc against a malicious software database.
- Protecting against phishing and malicious sites by checking visited websites against a threat intelligence database.

To turn on the Smart Screen, go to `Settings > Windows Security > App and Browser Control > Reputation-based Protection`. Scroll down and turn on the `SmartScreen option`.




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

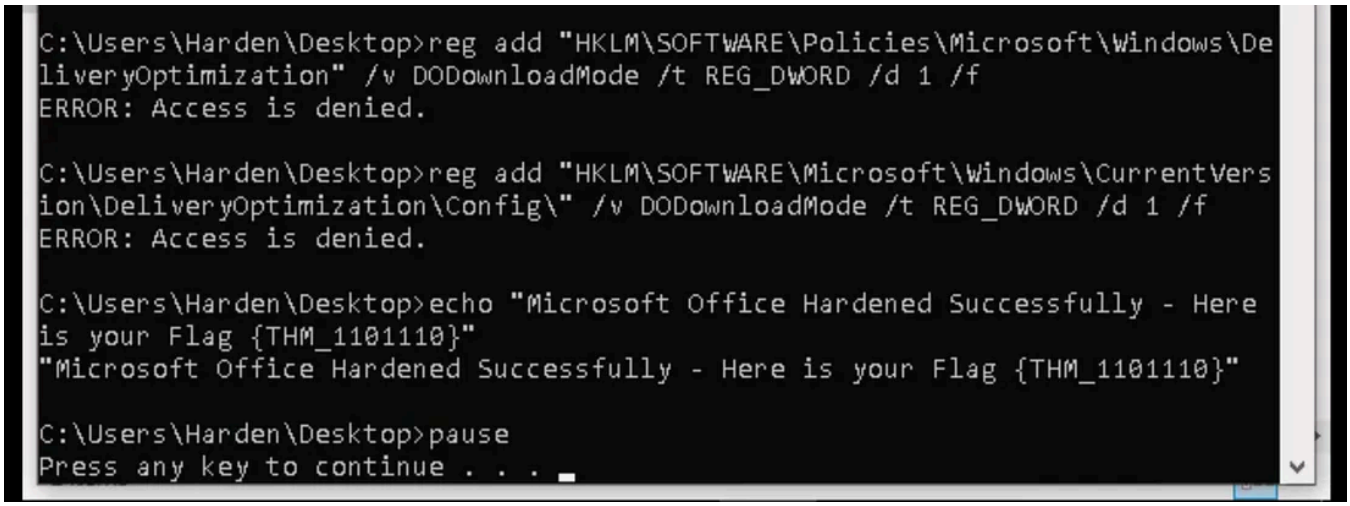



Answer: **.ps**

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

Answer: **Nay**

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




Answer: **{THM_1101110}**

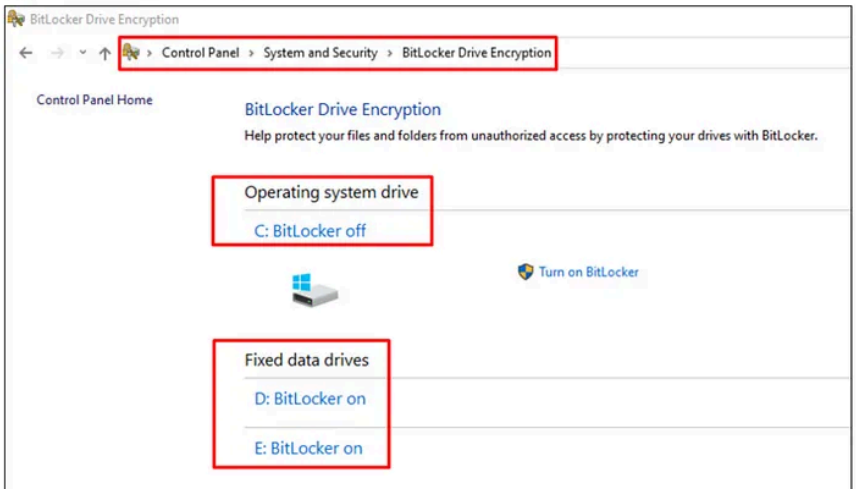
Task 6: **Storage Management**

### Data Encryption Through BitLocker

Encryption of the computer is one of the most vital things to which we usually pay little attention. The worst nightmare is that someone gets unfettered access to your devices' data. Encryption ensures that you or someone you share the recovery key with can access the stored content.

Microsoft, for its business edition of Windows, utilises the encryption tools by BitLocker. Let us have a quick look at how one can ensure to protect the data through BitLocker encryption features available on the Home Editions of Windows 10. You have already read about it here (Task 8).

Go to `Start > Control Panel > System and Security > BitLocker Drive Encryption`. You can easily see if the option to BitLocker Drive Encryption is enabled or not.



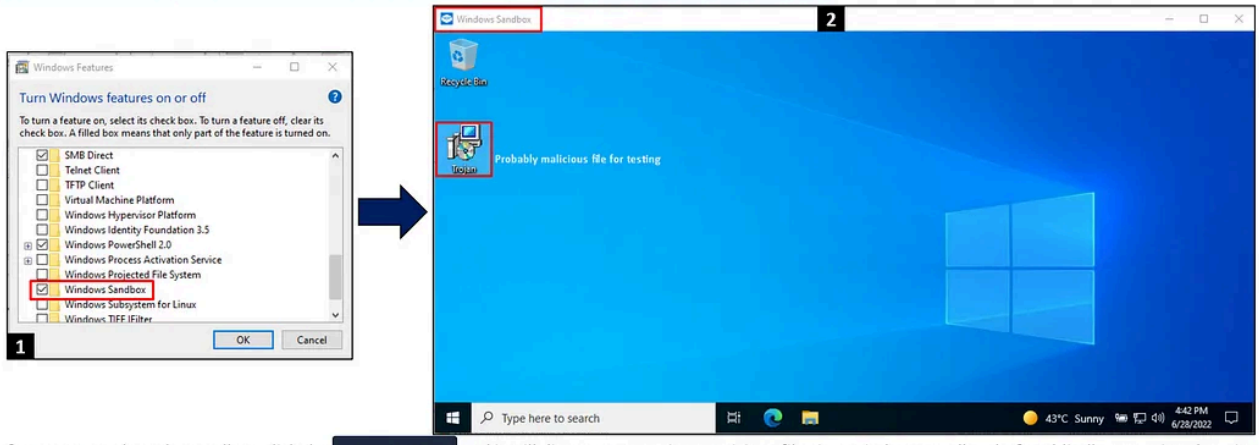

A trusted Platform Module chip TPM is one of the basic requirements to support BitLocker device encryption. Keeping the BitLocker recovery key in a secure place (preferably not on the same computer) is imperative. You can read more about BitLocker Recovery here.

**Note**: The BitLocker feature is not available in the attached VM.

### Windows Sandbox

To run applications safely, we can use a temporary, isolated, lightweight desktop environment called Windows Sandbox. We can install software inside this safe environment, and this software will not be a part of our host machine, it will remain sandboxed. Once the Windows Sandbox is closed, everything, including files, software, and states will be deleted. We would require Virtualisation enabled on our OS to run this feature. We cannot try this in the attached VM but the steps for enabling the Sandbox feature are as below:

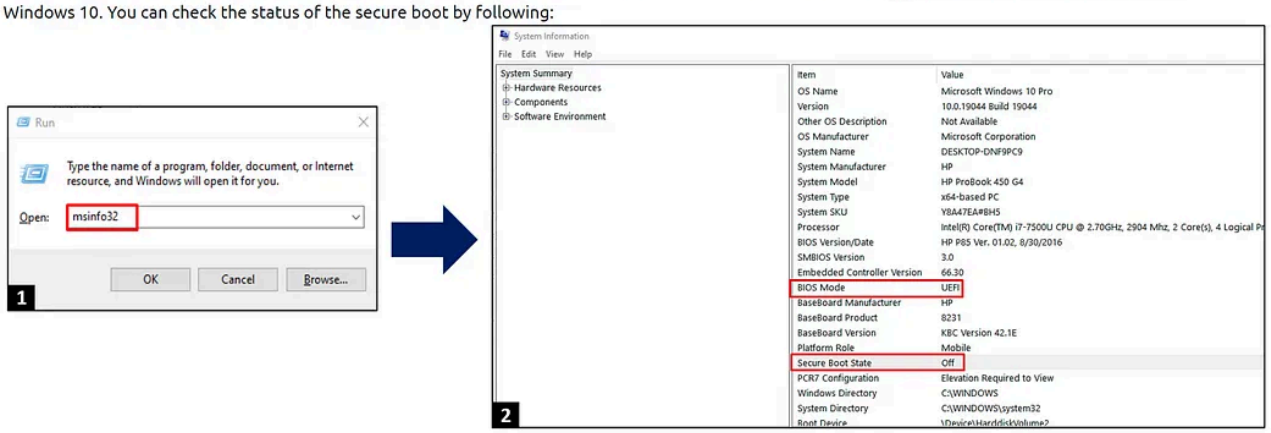
`Click Start > Search for 'Windows Features' and turn it on > Select Sandbox > Click OK to restart`




If you want to close the Sandbox, click the `close button,` and it will disappear. Opening suspicious files in a Windows Sandbox before blindly executing them in your base OS is recommended.

### Windows Secure Boot

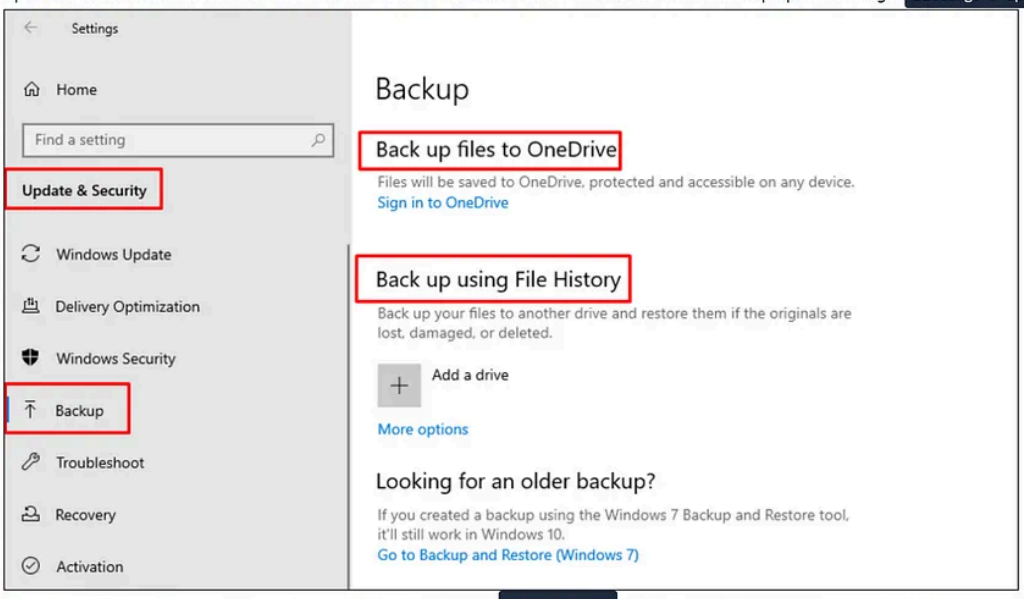
Secure boot – an advanced security standard - checks that your system is running on trusted hardware and firmware before booting, which ensures that your system boots up safely while preventing unauthorised software access from taking control of your PC, like malware.
You are already in a secure boot environment if you run a modern PC with Unified Extensible Firmware Interface UEFI (the best replacement for BIOS) or Windows 10. You can check the status of the secure boot by following:




The incredible thing is that you do not need to enable or install it as it works silently in the background. Windows allows you to disable these features, which is not recommended. You can enable Secure boot from BIOS settings (if disabled).

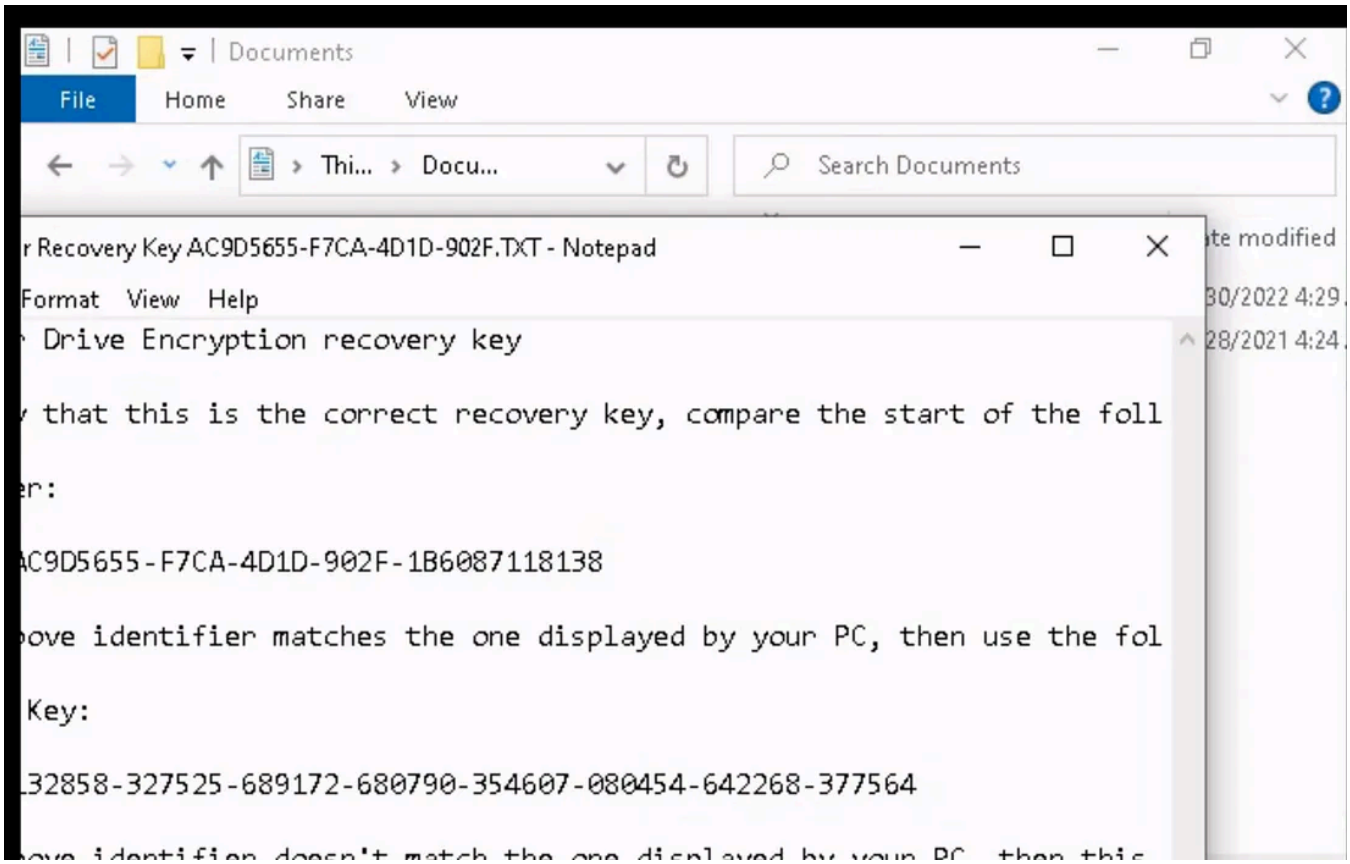
### Enable File Backups

The last option, but certainly not the least important one to prevent losing irreplaceable and critical files is to enable file backups. Despite all the above techniques, if you somehow lose essential data/files, you can recover the loss by restoring it, if you have a file backup option. Creating file backups is the best option to avoid disasters like malware attacks or hardware failure. You can enable the file backup option through `Settings > Update and Security > Backup` :-




Therefore, the most convenient option is enabling it from the '`File History`' option - a built-in functionality of Windows 10 and 11.

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?




Answer: **377564**

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

Answer: **48**

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

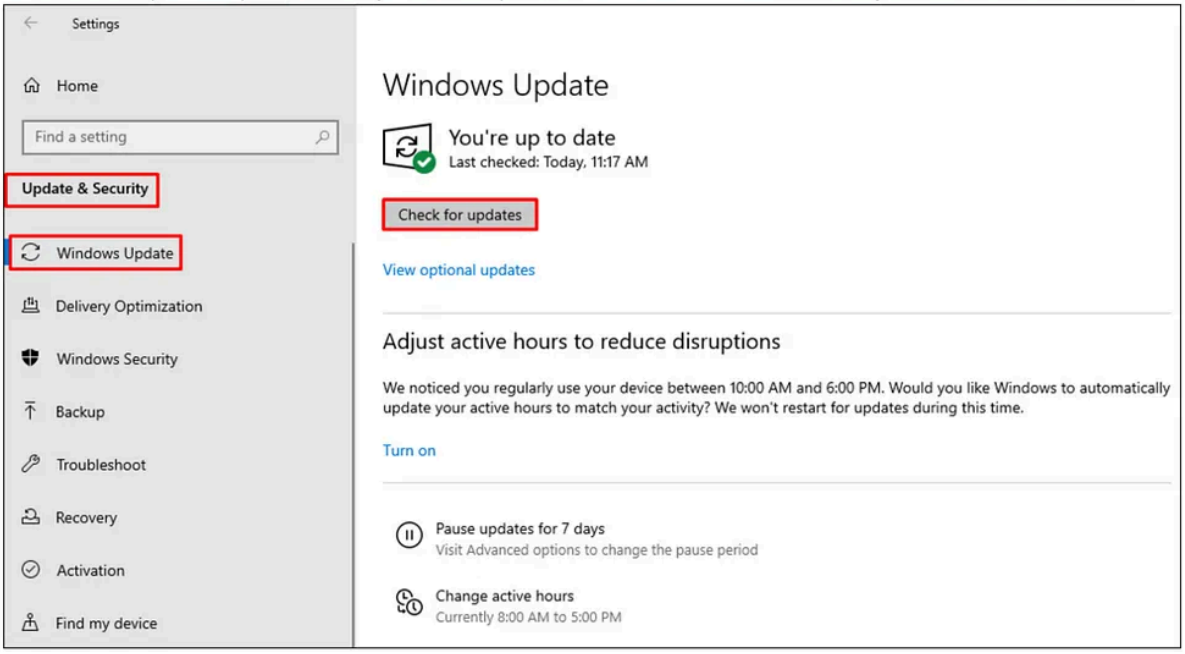

Answer: **.bkf**

Task 7: **Updating Windows**

Hackers are continuously bypassing and exploiting Windows' legitimate features. You can see a list of Windows vulnerabilities by following this link. The most critical part of hardening computers is enabling the Windows auto-updates.

```
Click Start > Settings > Update & Security > Window Updates.
```

This ensures that all the urgent security updates, if any, are installed immediately without causing any delay. It is most important because the quicker you apply the new Windows protection patch, the faster you can fix the potential vulnerabilities – to ensure the security from the latest known threats.




Remember, users who run the older Windows versions are always at greater risk and vulnerable to new security threats. So, be very careful about this.

**Microsoft Windows 10 : Security vulnerabilities, CVEs**

Security vulnerabilities of Microsoft Windows 10 : List of vulnerabilities affecting any version of this product

www.cvedetails.com

What is the CVE score for the vulnerability CVE ID CVE-2022–32230?

Exploit prediction scoring system (EPSS) score for CVE-2022-32230

Probability of exploitation activity in the next 30 days: 0.11%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 43 % EPSS Score History EPSS FAQ

CVSS scores for CVE-2022-32230

| Base Score | Base Severity | CVSS Vector | Exploitability Score | Impact Score | Source |
|---|---|---|---|---|---|
| 7.8 | HIGH | AV:N/AC:L/Au:N/C:N/I:N/A:C | 10.0 | 6.9 | nvd@nist.gov |
| 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H | 3.9 | 3.6 | cve@rapid7.con |
| 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H | 3.9 | 3.6 | nvd@nist.gov |

Answer: **7.8**

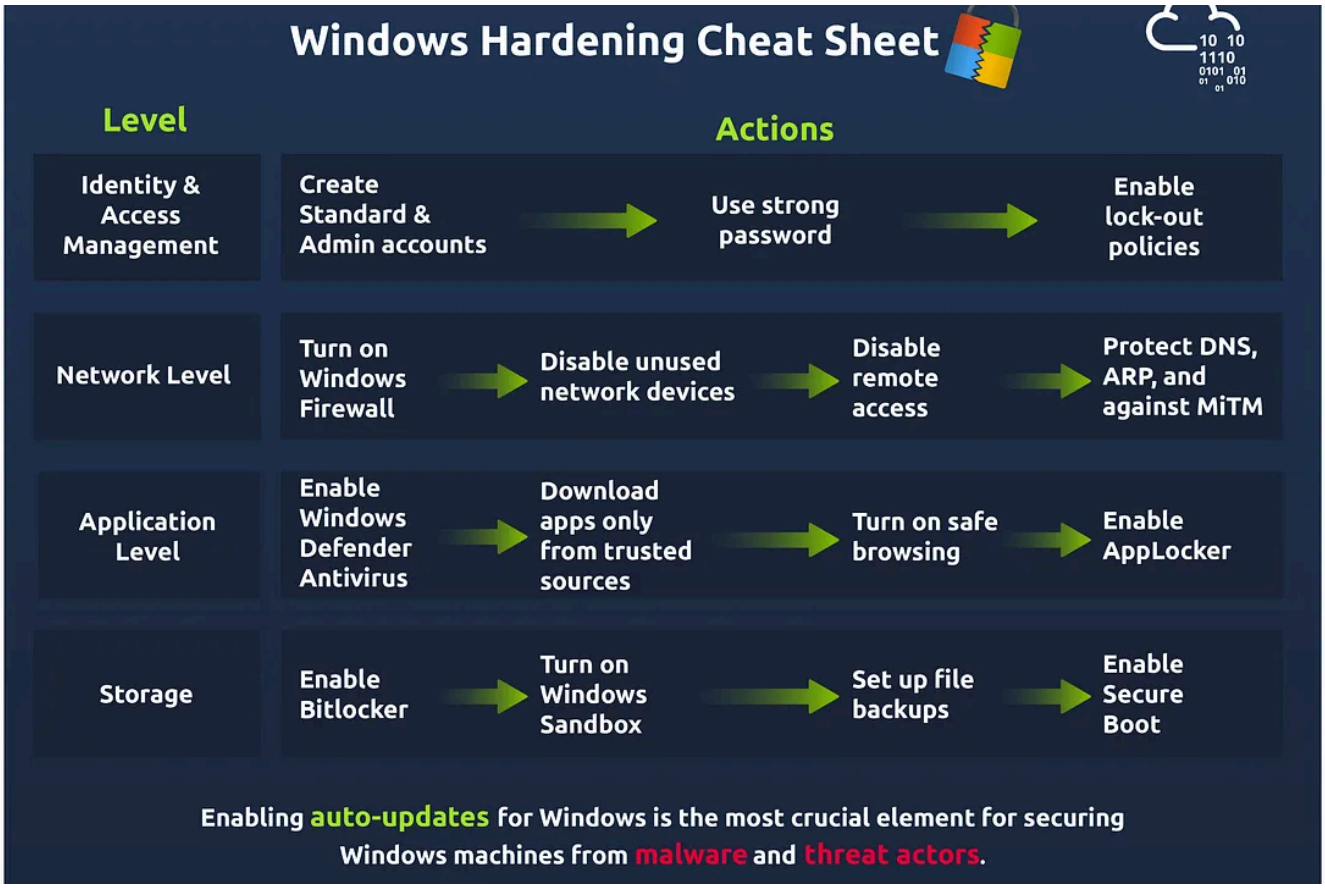
## Task 8: **Cheatsheet for Hardening Windows**

Is your system still at risk of a security breach?

Download Task Files

The bottom line is that hardening is a never-ending process. You can't ever say that your job is done and your system is now fully protected; instead, we can try our best. In this regard, we must be active and smart-minded to participate in this continuing process. We must keep in mind The defender's dilemma, which states that *breaches are inevitable because defenders have to be right 100% of the time whereas attackers only have to be right once.*

In this room, we have learned how to harden our computers at different levels (Identity, Network, Application & Storage). Below is a quick summary or cheatsheet for guidance during the hardening process:




Tryhackme Walkthrough | Tryhackme Writeup

Follow

## Written by Daniel Schwarzentraub

116 Followers · 4 Following

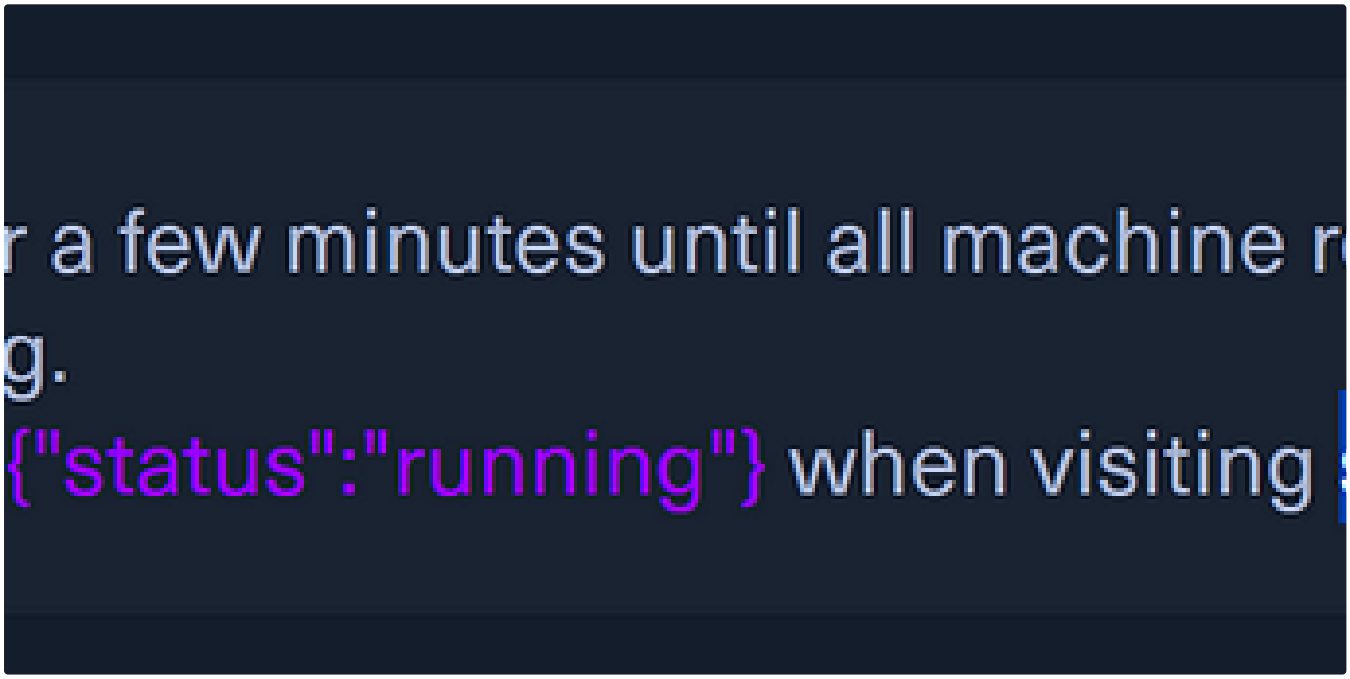
PNW_Hacker

## No responses yet

What are your thoughts?

Respond

## More from Daniel Schwarzentraub

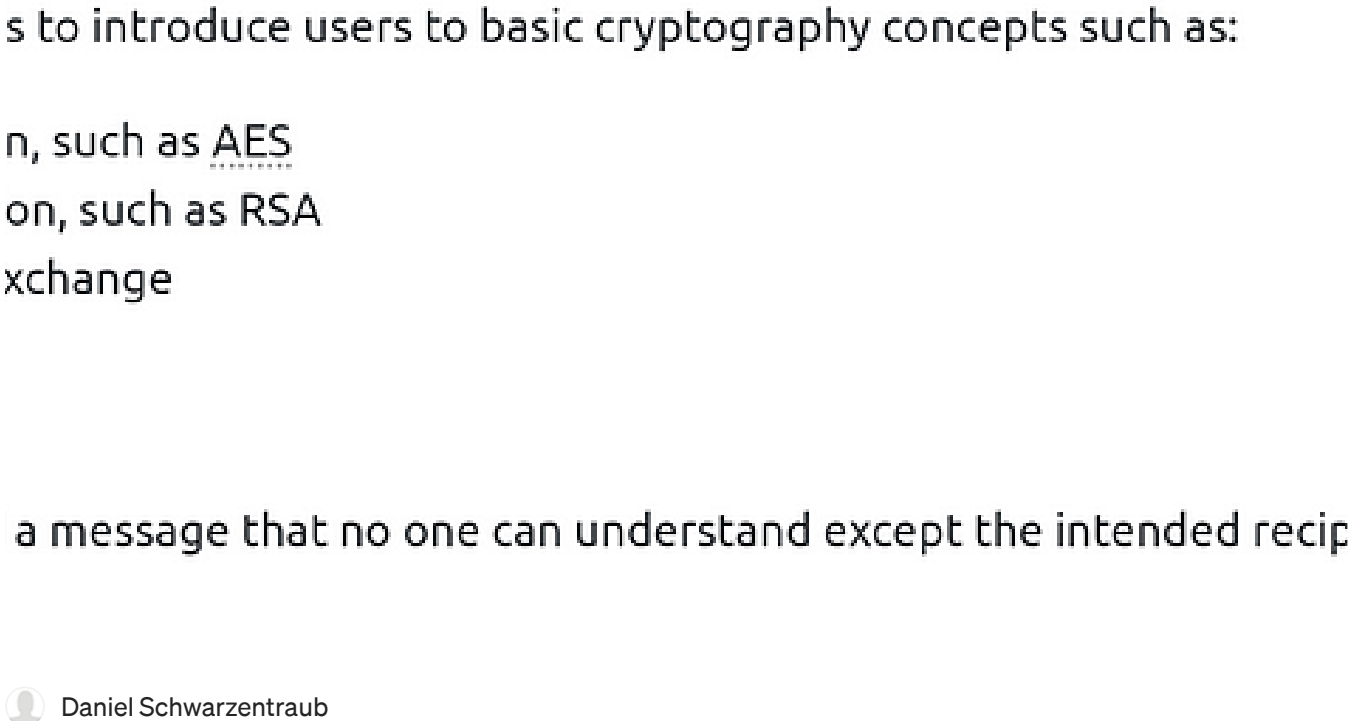



Daniel Schwarzentraub

### HTB—Tier 1 Starting Point: Three

HTB—Tier 1 Starting Point: Three

Jul 20, 2023 4 2

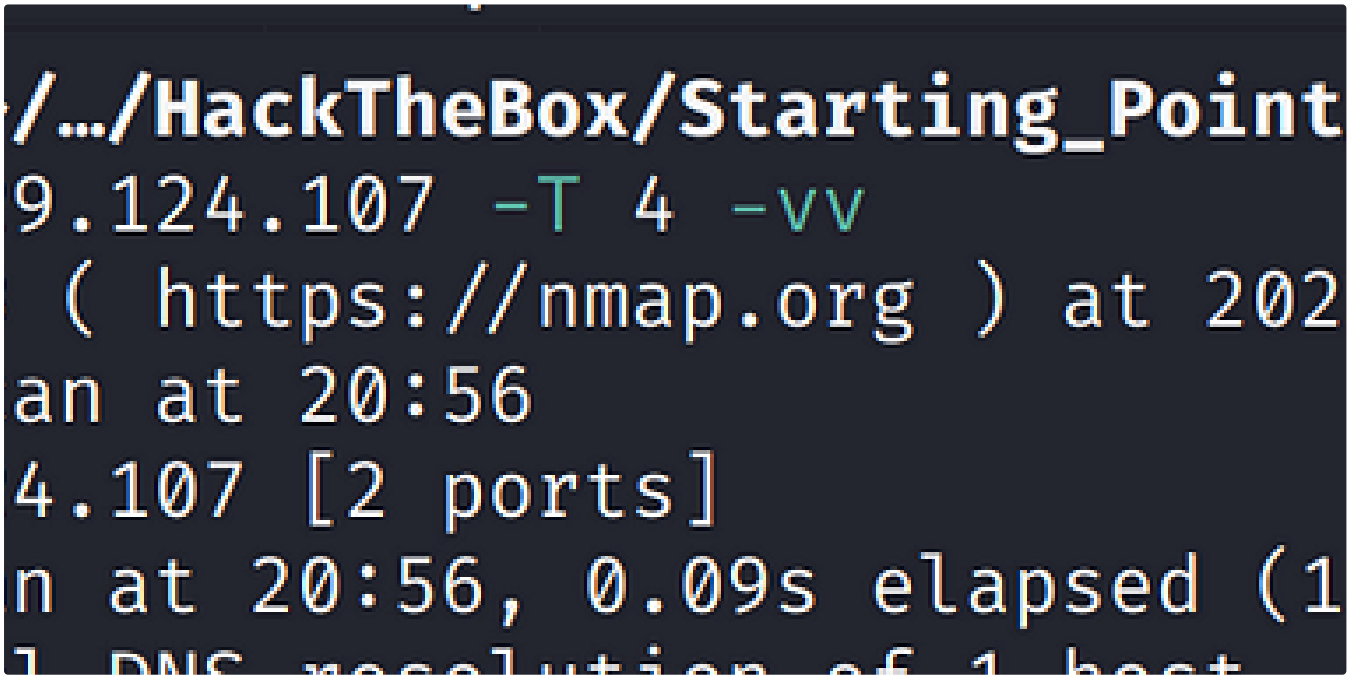



Daniel Schwarzentraub

## Tryhackme: Introduction to Cryptography

Tryhackme: Introduction to Cryptography

Sep 26, 2023 2




Daniel Schwarzentraub

## HTB—Tier 2 Starting Point: Archetype

HTB—Tier 2 Starting Point: Archetype

Jul 21, 2023

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 wa

Daniel Schwarzentraub

## Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

See all from Daniel Schwarzentraub

## Recommended from Medium


In T3CH by Axoloth

# TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

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 wa

Daniel Schwarzentraub

## Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

### Lists

**Staff picks**

796 stories · 1560 saves

**Stories to Help You Level-Up at Work**

19 stories · 912 saves

**Self-Improvement 101**

20 stories · 3196 saves

**Productivity 101**

20 stories · 2707 saves

rutbar

## TryHackMe—Search Skills | Cyber Security 101 (THM)

Evaluation of Search Results

Oct 26, 2024 1

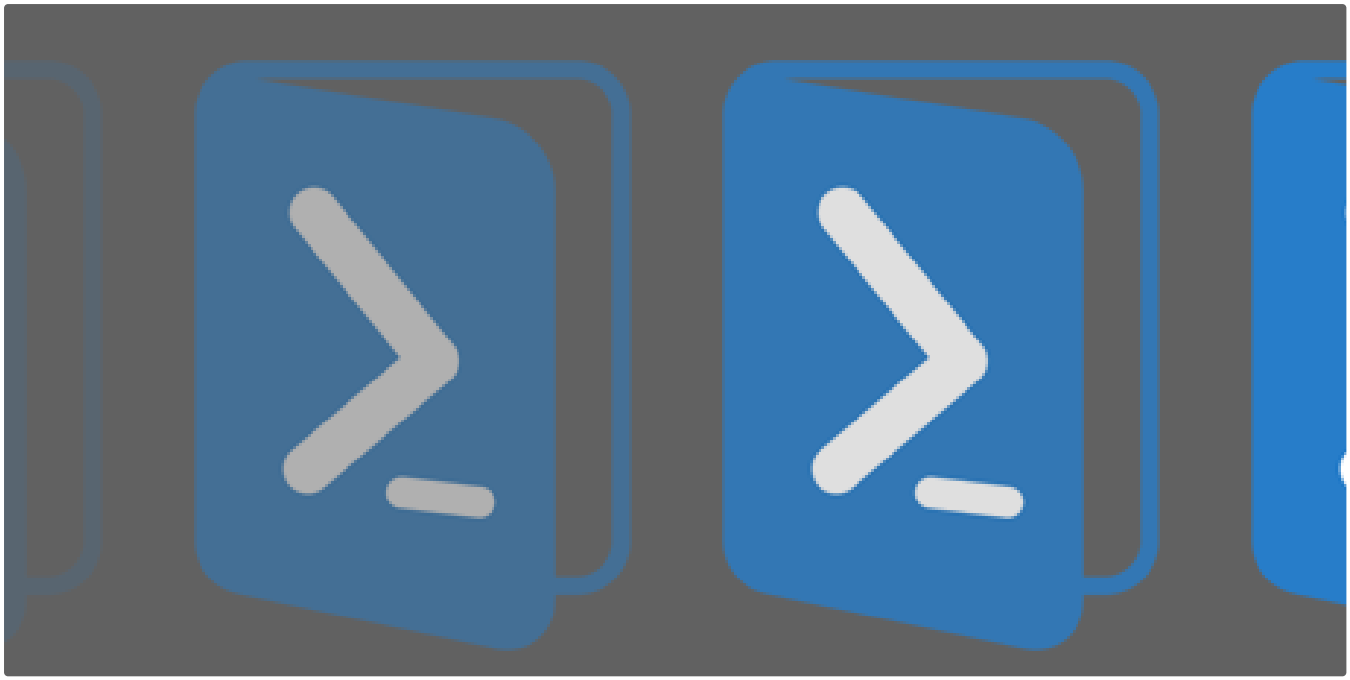


Trnty

## TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

Sep 7, 2024 10

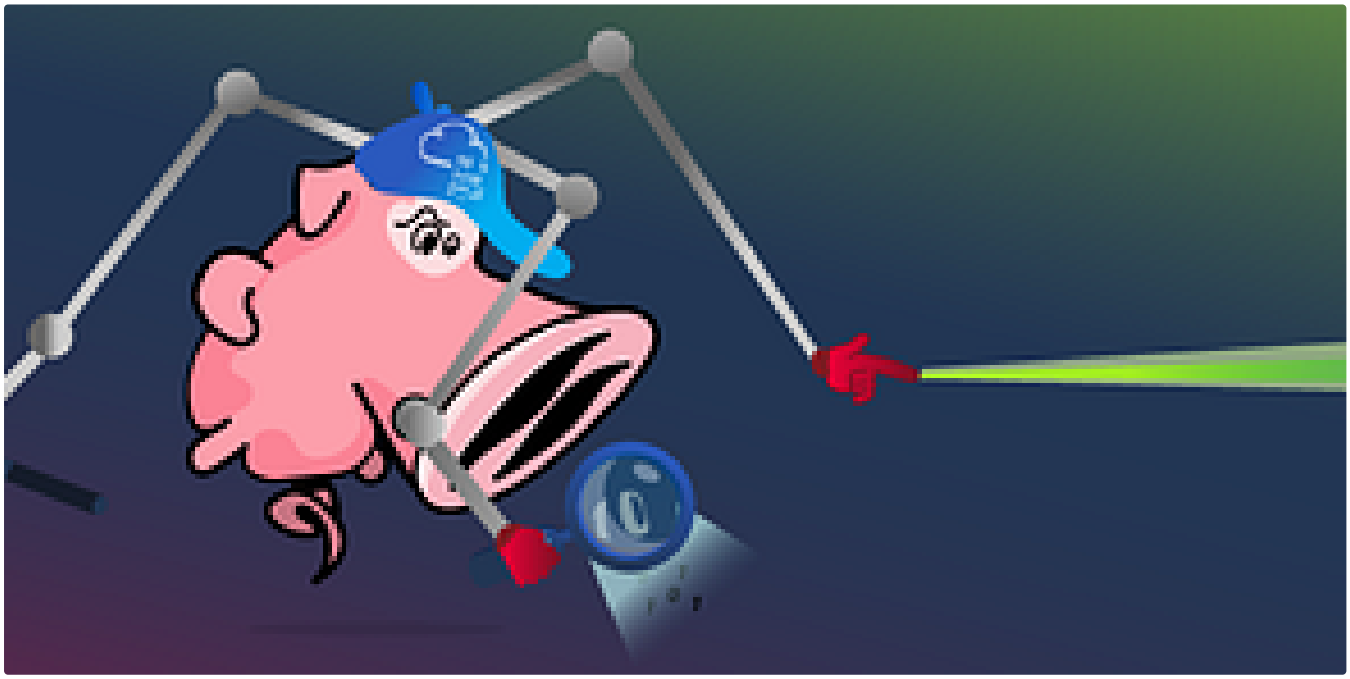


MatSec

## TryhackMe - Windows PowerShell | Cyber Security 101

Windows Powershell TryhackMe

Oct 24, 2024



In T3CH by Axoloth

## TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

Nov 9, 2024 100

See more recommendations