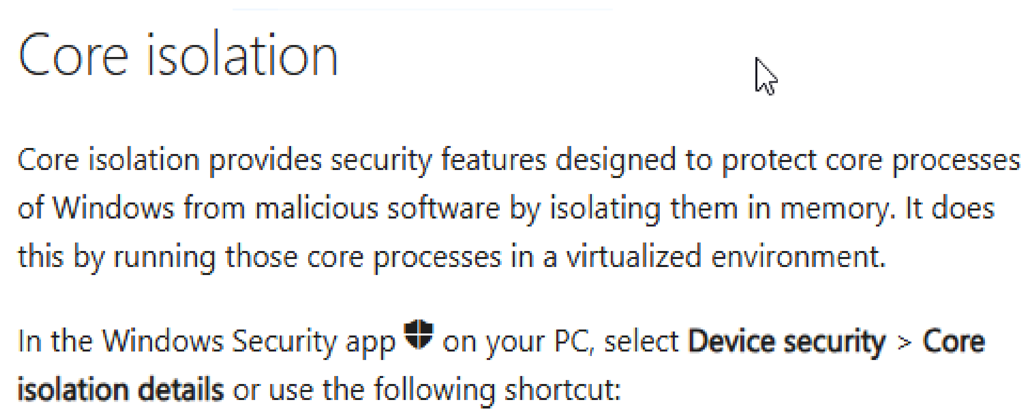
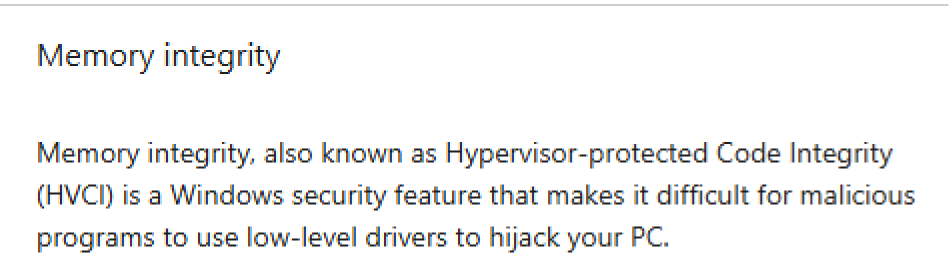
LAB1: EXPLORING SECURITY FEATURES AND FUNCTIONALITY



Core isolation

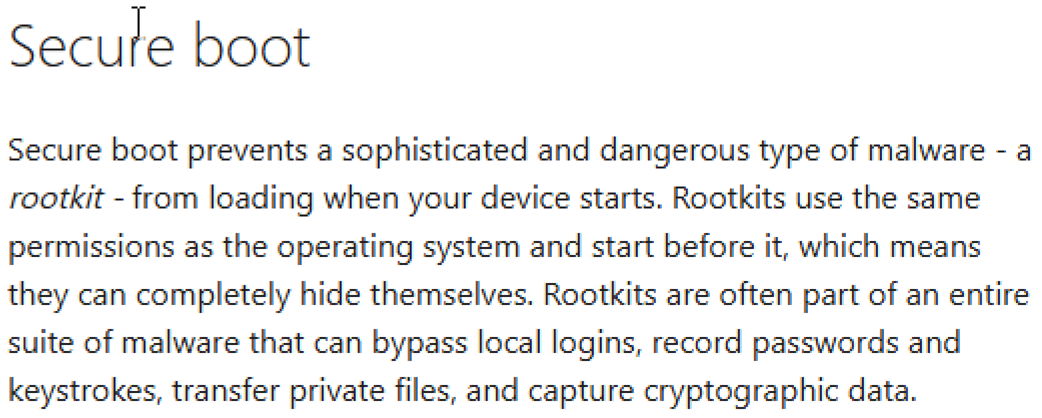
Core isolation provides security features designed to protect core processes of Windows from malicious software by isolating them in memory. It does this by running those core processes in a virtualized environment.

In the Windows Security app 🛡 on your PC, select **Device security** > **Core isolation details** or use the following shortcut:



Memory integrity

Memory integrity, also known as Hypervisor-protected Code Integrity (HVCI) is a Windows security feature that makes it difficult for malicious programs to use low-level drivers to hijack your PC.



Secure boot

Secure boot prevents a sophisticated and dangerous type of malware - a *rootkit* - from loading when your device starts. Rootkits use the same permissions as the operating system and start before it, which means they can completely hide themselves. Rootkits are often part of an entire suite of malware that can bypass local logins, record passwords and keystrokes, transfer private files, and capture cryptographic data.

TPM (Trusted Platform Module) is a **dedicated security chip** built into most modern computers.
It’s designed to **securely store cryptographic keys, passwords, and certificates**, making your device more resistant to attacks.

Feature	**How TPM Helps**
Core Isolation	Verifies trusted boot and helps secure virtualization features.
BitLocker	Stores encryption keys securely in TPM, so you don’t need a USB key or password at every startup.
Windows Hello / PIN	Protects credentials using TPM hardware.
Secure Boot	Ensures system integrity from power-on.

LINUX:

Firewall check;

IPTABLES AND NFTABLES

AppArmor Status:

```
apparmor module is loaded.
1 profiles are loaded.
1 profiles are in enforce mode.
   docker-default
0 profiles are in complain mode.
0 profiles are in prompt mode.
0 profiles are in kill mode.
0 profiles are in unconfined mode.
0 processes have profiles defined.
0 processes are in enforce mode.
0 processes are in complain mode.
0 processes are in prompt mode.
```

```
0 processes are in kill mode.

0 processes are unconfined but have a profile defined.

0 processes are in mixed mode.
```

LAB2: IDENTIFYING SECURITY BUGS AND VULNERABLITY

CVE ID: CVE-2025-8556   -RED HAT

Description

A flaw was found in CIRCL's implementation of the FourQ elliptic curve. This vulnerability allows an attacker to compromise session security via low-order point injection and incorrect point validation during Diffie-Hellman key exchange.

SEVERITY: LOW

MITIGATION: Upgrade CIRCL to v1.6. or newer. This version includes patches for the invalid/low order point validation, correct unmarshall and improved checks.

CVE-2025-59502 - MICROSOFT CORPORATION

Description

Uncontrolled resource consumption in Windows Remote Procedure Call allows an unauthorized attacker to deny service over a network.

SEVERITY: HIGH

MITIGATION: Apply Microsoft's security Update (October 2025). It helps the vendor patch resolves the underlying resources exhaustion flaw.

WINDOW POWERSHELL- INSTALLED UPDATES

```
PS C:\Users\aibuk> Get-Hotfix


Source      Description     HotFixID     InstalledBy        InstalledOn
```

```
------      -----------     --------     -----------       -----------

DESKTOP-K9... Update        KB5066130    NT AUTHORITY\SYSTEM  10/22/2025 12:00:00
AM

DESKTOP-K9... Update        KB4577586                   7/11/2021 12:00:00 AM

DESKTOP-K9... Security Update  KB4580325                   7/11/2021 12:00:00 AM

DESKTOP-K9... Update        KB4589212                   7/11/2021 12:00:00 AM

DESKTOP-K9... Update        KB5007401                   7/11/2021 12:00:00 AM

DESKTOP-K9... Update        KB5011048                   7/11/2021 12:00:00 AM

DESKTOP-K9... Update        KB5011069                   7/11/2021 12:00:00 AM

DESKTOP-K9... Update        KB5015684                   7/11/2021 12:00:00 AM

DESKTOP-K9... Update        KB5021043                   7/11/2021 12:00:00 AM

DESKTOP-K9... Update        KB5023319                   7/11/2021 12:00:00 AM

DESKTOP-K9... Security Update  KB5066791    NT AUTHORITY\SYSTEM  10/16/2025
12:00:00 AM

DESKTOP-K9... Update        KB5020372                   7/11/2021 12:00:00 AM

DESKTOP-K9... Update        KB5031539    NT AUTHORITY\SYSTEM  10/17/2023 12:00:00
AM

DESKTOP-K9... Update        KB5031540    NT AUTHORITY\SYSTEM  11/7/2023 12:00:00 AM

DESKTOP-K9... Update        KB5032392    NT AUTHORITY\SYSTEM  11/29/2023 12:00:00
AM

DESKTOP-K9... Update        KB5032907    NT AUTHORITY\SYSTEM  1/2/2024 12:00:00 AM

DESKTOP-K9... Update        KB5034224    NT AUTHORITY\SYSTEM  2/23/2024 12:00:00 AM

DESKTOP-K9... Update        KB5036447    NT AUTHORITY\SYSTEM  3/23/2024 12:00:00 AM

DESKTOP-K9... Security Update  KB5037018    NT AUTHORITY\SYSTEM  4/24/2024 12:00:00
AM

DESKTOP-K9... Update        KB5037240    NT AUTHORITY\SYSTEM  5/25/2024 12:00:00 AM

DESKTOP-K9... Update        KB5037995    NT AUTHORITY\SYSTEM  6/15/2024 12:00:00 AM
```

```
DESKTOP-K9... Update          KB5039336     NT AUTHORITY\SYSTEM  7/13/2024 12:00:00 AM
DESKTOP-K9... Security Update  KB5041579     NT AUTHORITY\SYSTEM  8/18/2024 12:00:00 AM
DESKTOP-K9... Security Update  KB5043935     NT AUTHORITY\SYSTEM  9/19/2024 12:00:00 AM
DESKTOP-K9... Update          KB5043130     NT AUTHORITY\SYSTEM  10/16/2024 12:00:00 AM
DESKTOP-K9... Update          KB5046823     NT AUTHORITY\SYSTEM  11/18/2024 12:00:00 AM
DESKTOP-K9... Security Update  KB5050388     NT AUTHORITY\SYSTEM  1/17/2025 12:00:00 AM
DESKTOP-K9... Update          KB5050111     NT AUTHORITY\SYSTEM  2/16/2025 12:00:00 AM
DESKTOP-K9... Update          KB5052916     NT AUTHORITY\SYSTEM  3/14/2025 12:00:00 AM
DESKTOP-K9... Update          KB5054682     NT AUTHORITY\SYSTEM  4/12/2025 12:00:00 AM
DESKTOP-K9... Security Update  KB5058526     NT AUTHORITY\SYSTEM  5/14/2025 12:00:00 AM
DESKTOP-K9... Update          KB5059504     NT AUTHORITY\SYSTEM  6/15/2025 12:00:00 AM
DESKTOP-K9... Security Update  KB5063706     NT AUTHORITY\SYSTEM  7/13/2025 12:00:00 AM
DESKTOP-K9... Update          KB5063261     NT AUTHORITY\SYSTEM  8/16/2025 12:00:00 AM
DESKTOP-K9... Update          KB5063979     NT AUTHORITY\SYSTEM  9/10/2025 12:00:00 AM
DESKTOP-K9... Security Update  KB5066790     NT AUTHORITY\SYSTEM  10/16/2025 12:00:00 AM
DESKTOP-K9... Update          KB5004393                          7/11/2021 12:00:00 AM
```

LOCAL PORT SCAN:

```
nmap -sS 127.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-30 22:32 EDT
```

```
Nmap scan report for localhost (127.0.0.1)

Host is up (0.0000090s latency).

All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.

Not shown: 1000 closed tcp ports (reset)


Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

LAB 3: PRIVACY AND TELEMENTRY CONTROL

By configuring this setting in Windows 10, end users will not be able to opt into a higher level of telemetry collection than the level you have set for your organization. This limitation applies only to the Windows operating system and apps included with Windows, and does not apply to third-party apps running on Windows 10.

Diagnostic data is categorized into four levels, as follows:

- 0 (Security). Information that's required to help keep Windows, Windows Server, and System Center secure, including data about the Connected User Experiences and Telemetry component settings, the Malicious Software Removal Tool, and Windows Defender.

- 1 (Required). Basic device info, including: quality-related data, app compatibility, and data from the Security level.

- 2 (Enhanced). Additional insights, including: how Windows, Windows Server, System Center, and apps are used, how they perform, advanced reliability data, and data from both the Required and the Security levels.

- 3 (Optional). All data necessary to identify and help to fix problems, plus data from the Security, Required, and Enhanced levels.

Options available to users in the Settings app are changed by configuring this setting, and even if not set, may be impacted by other group policy settings. Note that if this policy is configured to allow a telemetry setting of Security or Basic, end users will be unable to select a higher level

LAB4: LINUX SECURITY AND HARDENING

1. Update System Packages

```
sudo apt update && sudo apt upgrade -y
```

Explanation:
Keeping packages up-to-date ensures the system has the latest security patches and removes known vulnerabilities that attackers could exploit.

2. Enable and Configure the Firewall (UFW)

```
sudo apt install ufw -y

sudo ufw enable
```

Explanation:
UFW (Uncomplicated Firewall) restricts unauthorized network access by allowing only necessary ports (like SSH) and denying everything else by default.

---

3. Disable Direct Root Login over SSH

```
sudo nano /etc/ssh/sshd_config

# Change or add:
```

```
PermitRootLogin no
```

```
sudo systemctl restart ssh
```

Explanation:
Prevents remote attackers from attempting to brute-force or directly access the root account, forcing logins through regular users who use sudo when required.

Check Active Services

```
sudo systemctl list-units --type=service
```

Explanation:
Listing running services helps identify unnecessary or insecure daemons that can be disabled to reduce the attack surface.

---

4. Enable Automatic Security Updates

```
sudo apt install unattended-upgrades -y
```

```
sudo dpkg-reconfigure --priority=low unattended-upgrades
```

Explanation:
Automatically installs security patches without user intervention, ensuring critical vulnerabilities are fixed promptly.

5. Create a non-root user and add to sudo group:

```
Sudo adduser student
```

```
Sudo usermod -aG sudo student
```

Explanation:

Using a non-root user for daily operations limits damage if the account is compromised. Adding to the sudo group allows controlled privilege escalation only when needed.

Summary:
These hardening steps collectively minimize exposure to external attacks, enforce the principle of least privilege, and maintain a secure and stable Linux environment.

LAB5: USING ANONYMITY-FOCUSED OS (TAILS/WHONIX)

1. Tails prevents data persistence by design — it's built so that everything you do leaves no trace once you shut it down or remove the USB.

2. **Whonix-Gateway** Handles all internet traffic through the **Tor network**. It is also what allows you to actually browse, use apps, etc.. You can't be completely isolated from the internet except through the Gateway.

3. Journalists working under surveillance or censorship.
   Whistleblowers.
   Everyday users who want privacy on shared/public systems.
   Activists

LAB6: PENETRATION TESTING OS(KALI LINUX)

1) Reconnaissance / Information Gathering

- **Nmap**
- **Masscan**

- **theHarvester, OSINT tools**

Purpose: map the attack surface, discover hosts, services, and public info.

---

2) Enumeration & Scanning

- **Nikto** —
- **Gobuster / DirBuster**
- **Nmap NSE scripts** —

Purpose: find web directories, available services, weak configurations.

---

3) Vulnerability Assessment

- **OpenVAS / Greenbone / Nessus**
- **sqlmap** .

Purpose: discover known CVEs, misconfigurations, or injection points.

---

4) Exploitation Frameworks (use only with explicit authorization)

- **Metasploit Framework**
- **BeEF**

Purpose: verify that discovered vulnerabilities are actually exploitable (proof-of-concept.

Definition of Ethical Hacking- Ethical hacking is the legal and authorized process of testing computer systems, networks, or applications to find and fix security weaknesses before malicious hackers can exploit them.