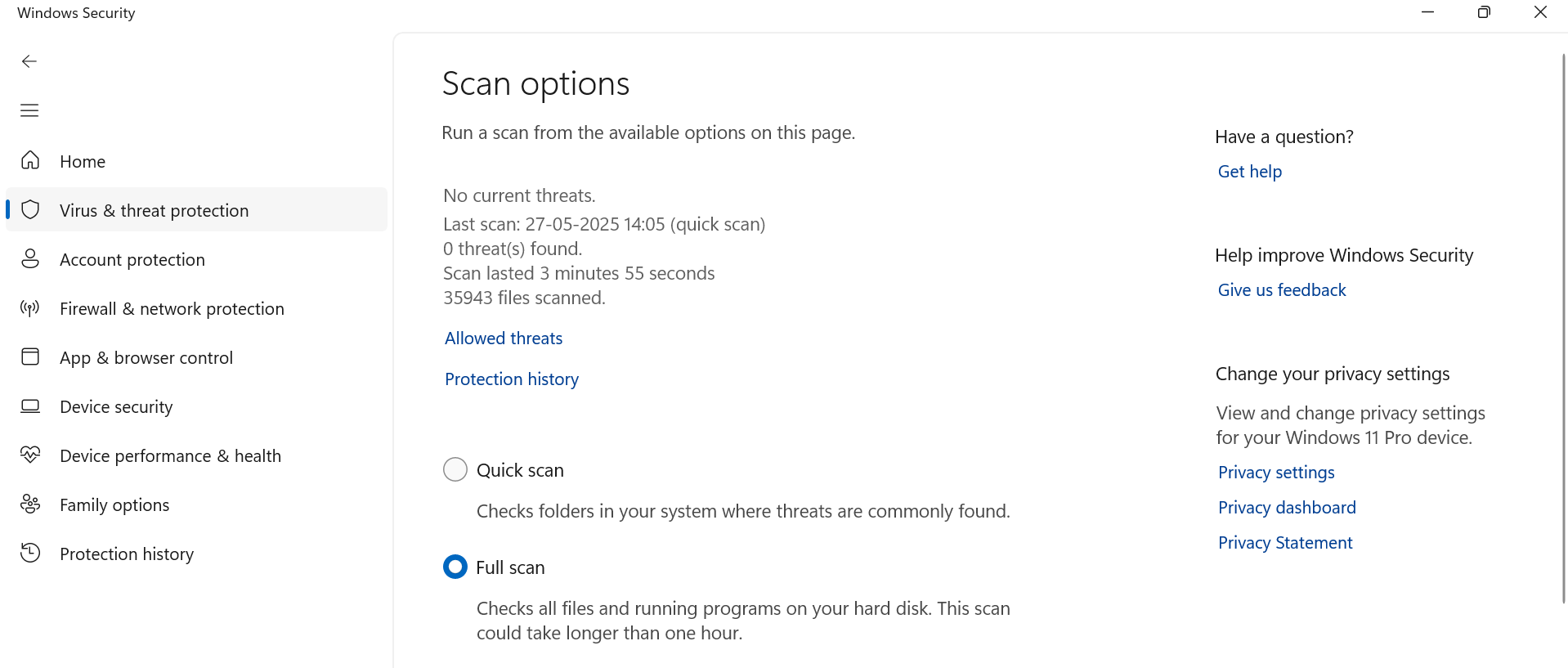
**Task 3 : Perform a Basic Vulnerability Scan on Your PC.**

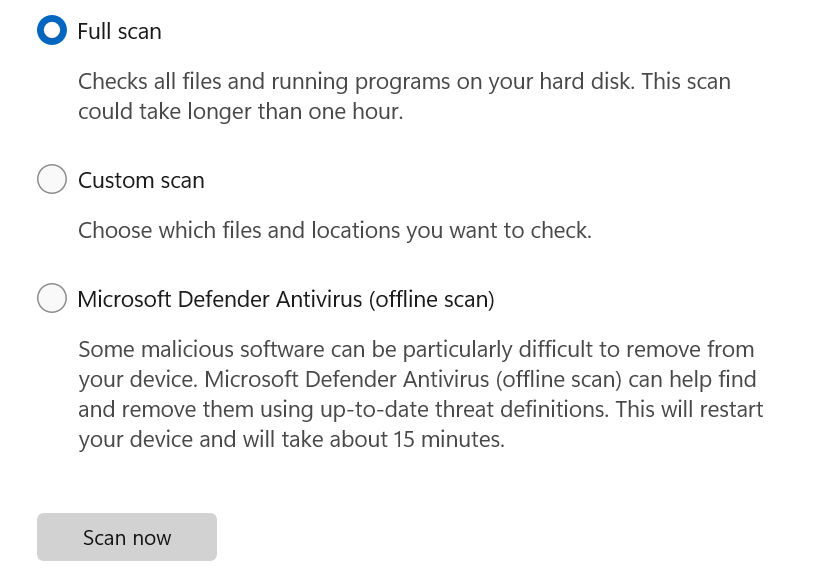
**Objective:** Use free tools to identify common vulnerabilities on your computer.

**Tools:** OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials.

**Deliverables:** Vulnerability scan report with identified issues.

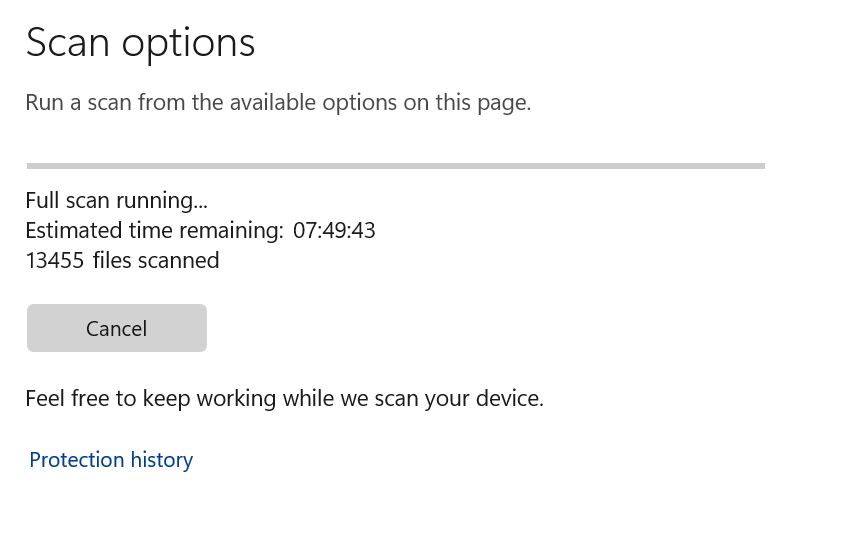
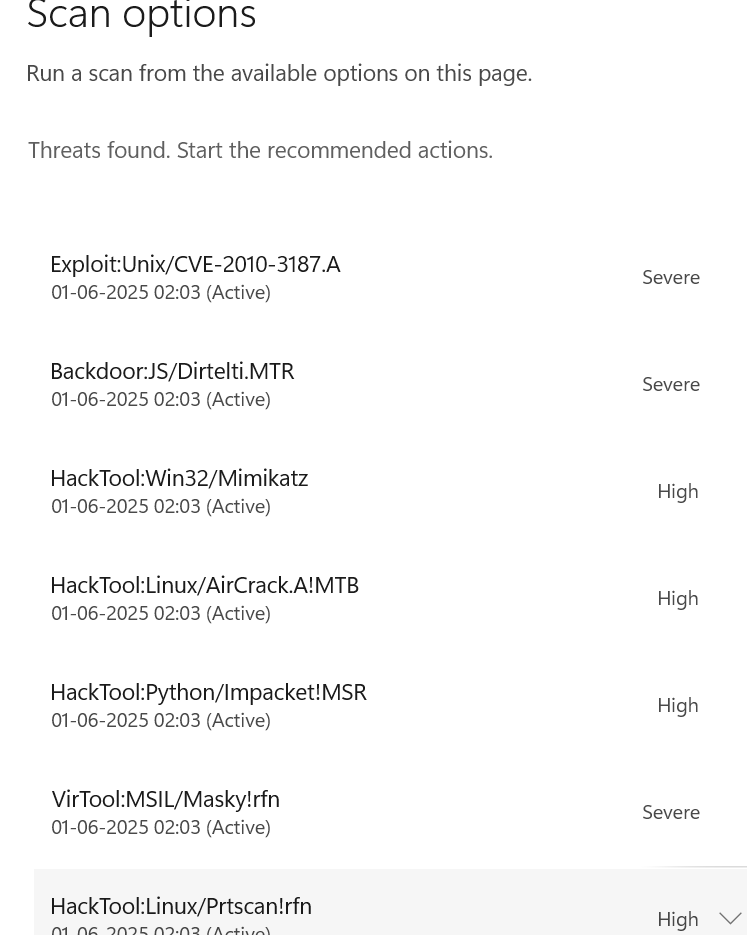
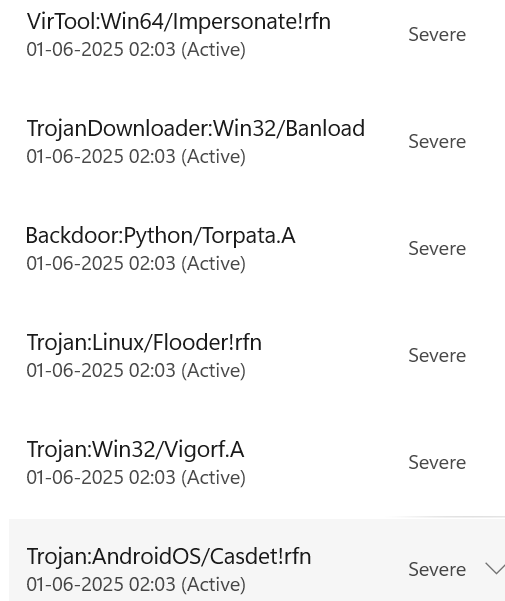
**1. Install OpenVAS or Nessus Essentials.**

**2. Set up scan target as your local machine IP or localhost.**   
Here using WINDOWS BUILT-IN “Virus & Threat Protection”.

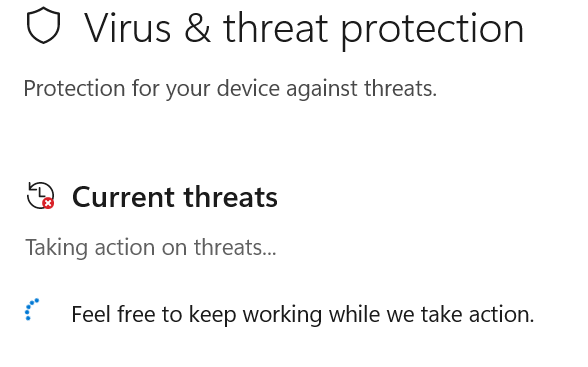


**3. Start a full vulnerability scan.**

**4. Wait for scan to complete (may take 30-60 mins).**

**5. Review the report for vulnerabilities and severity.**

**6. Research simple fixes or mitigations for found vulnerabilities.**

****

**a) Exploit:** Simple fixes and mitigation strategies include regularly patching software and operating systems, implementing strong access control, and educating employees on safe computing habits. Additionally, monitoring for suspicious activity and leveraging multi-factor authentication can help minimize the impact.

**b)** **Backdoor:** To fix or mitigate backdoor attacks, focus on hardening your system security, implementing strong access controls, and regularly scanning for malicious activity. Keep software and operating systems up-to-date, use strong passwords and two-factor authentication, and consider utilizing firewalls and intrusion detection systems.

**c)** **Hacktool:** To mitigate hacktool threats, implement multi-factor authentication, network segmentation, and strong password policies. Regularly update software and plugins, and conduct security audits to identify vulnerabilities. Employee training on social engineering tactics is also crucial.

**d) VirTool:** To mitigate cybersecurity risks like those posed by "Virtool", focus on strong password policies, software updates, and user awareness training. Additionally, implement endpoint detection and response tools and consider network segmentation to isolate potential breaches.

**e)** **Trojan:** To address a Trojan infection, immediately disconnect the device from the internet and boot into Safe Mode to limit the Trojan's functionality. Then, install and update reputable antivirus software and run a full system scan to detect and remove the Trojan. After removal, change passwords, monitor financial accounts, and practice safe browsing habits.

**7. Document the most critical vulnerabilities.**

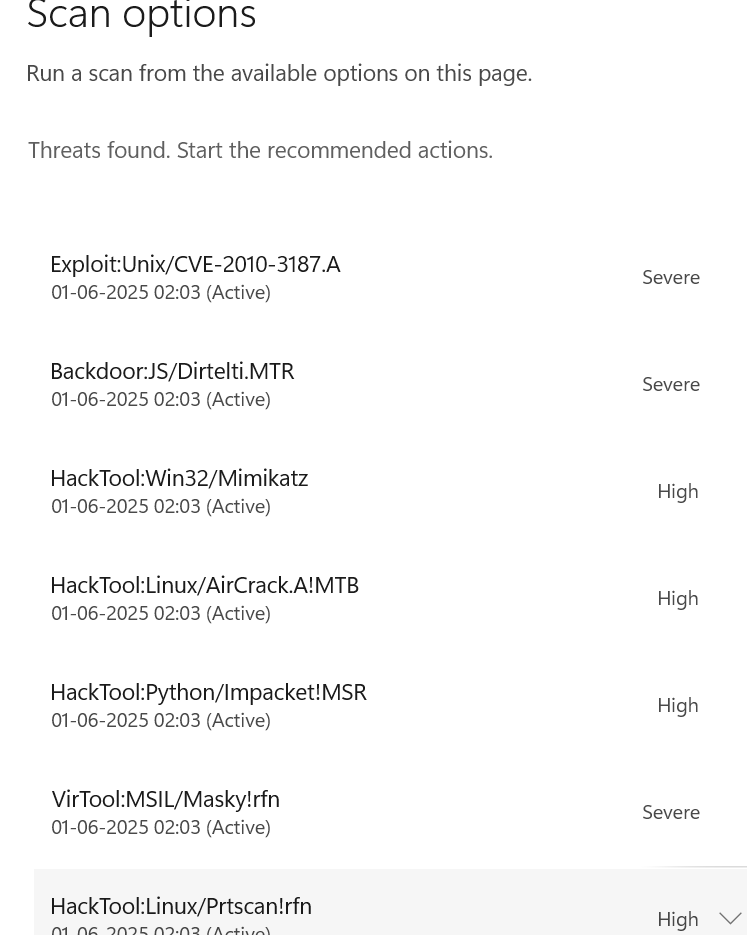
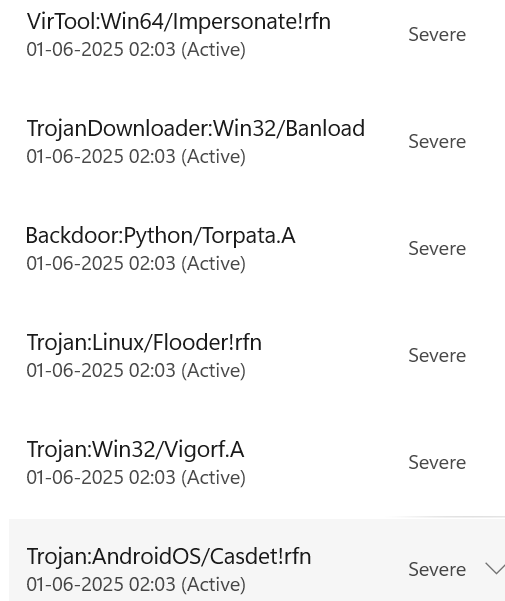
**a) Exploit:** In cybersecurity, an exploit is a method or piece of code that takes advantage of a vulnerability in software, hardware, or network to cause harm, such as installing malware or disrupting services.

**b)** **Backdoor:** In cybersecurity, a backdoor is a hidden entry point that bypasses a system's normal security measures, potentially allowing unauthorized access. These backdoors can be introduced intentionally by developers or maliciously by attackers, creating a vulnerability that can be exploited for various malicious purposes.

**c)** **Hacktool:** In cybersecurity, "hacktool" refers to a category of tools or software that, while not strictly malicious, can pose a risk to users by potentially being used for unauthorized access or system manipulation. These tools are often used for security testing or research but can also be used by malicious actors to exploit vulnerabilities.

**d)** **VirTool:** In cybersecurity, "VirTool" typically refers to a detection name used by antivirus and anti-malware software, indicating a program that has been obfuscated or modified to evade detection. It's often associated with riskware/ tools used to create or modify malware, making it more difficult to analyze and detect.

**e)** **Trojan:** In cybersecurity, a Trojan horse is a type of malware that disguises itself as a legitimate program or software, often to trick users into running it.

 **8. Take screenshots of the scan results.**