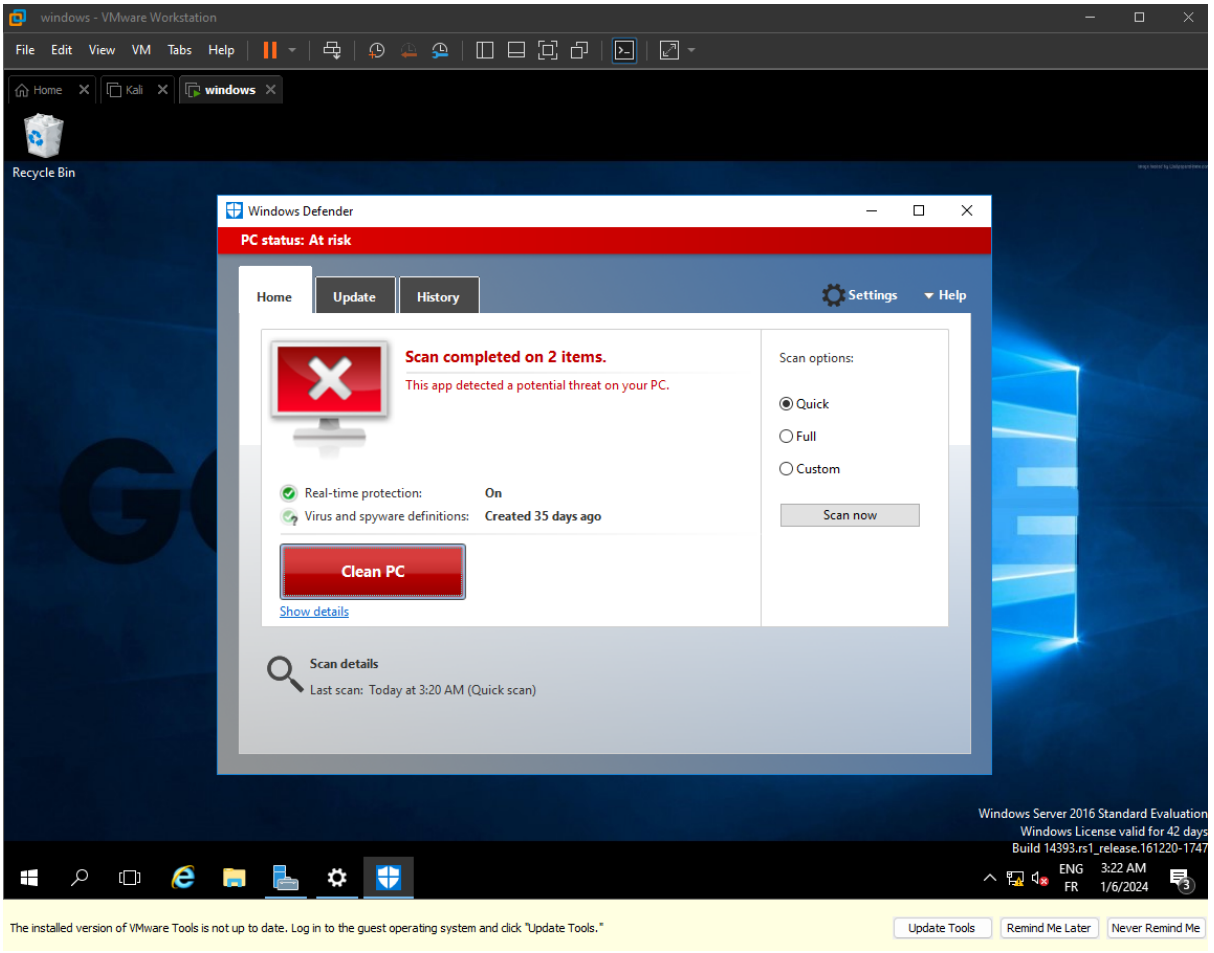
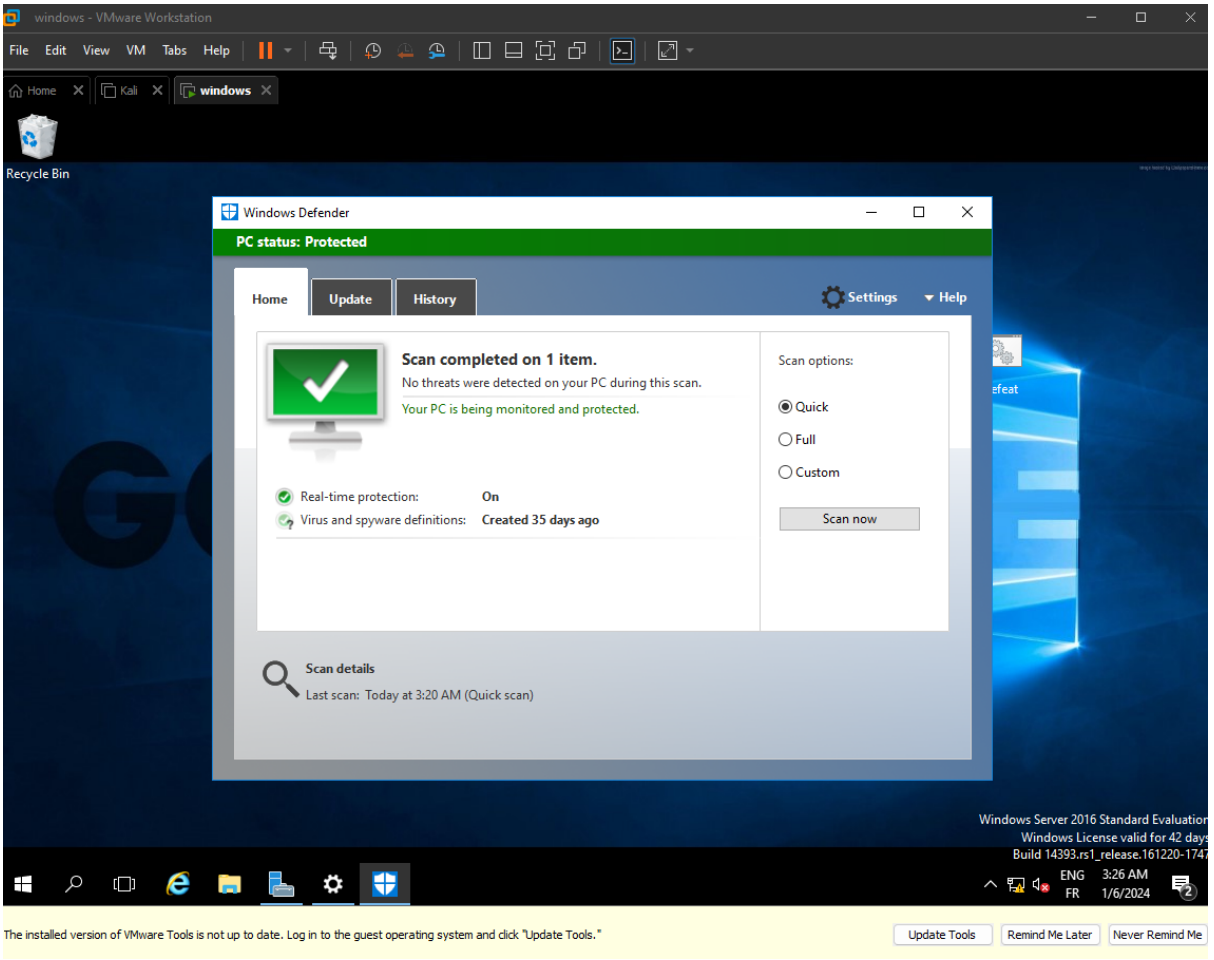
Checkpoint attack, threat

- First download the following folder: link
- login to the Windows server : Administrator : Gomycode01*
- copy the try_and_run_me.ps1 inside the Windows server
- Does Windows Defender take action?
- If yes, why ?? (correct answer: detection of possible trojan)
- if no: right click on the file and run Windows Defender analysis
- What is the reaction of windows ? https://i.imgur.com/0ff8fT6.png

https://i.imgur.com/6gQSLDX.png



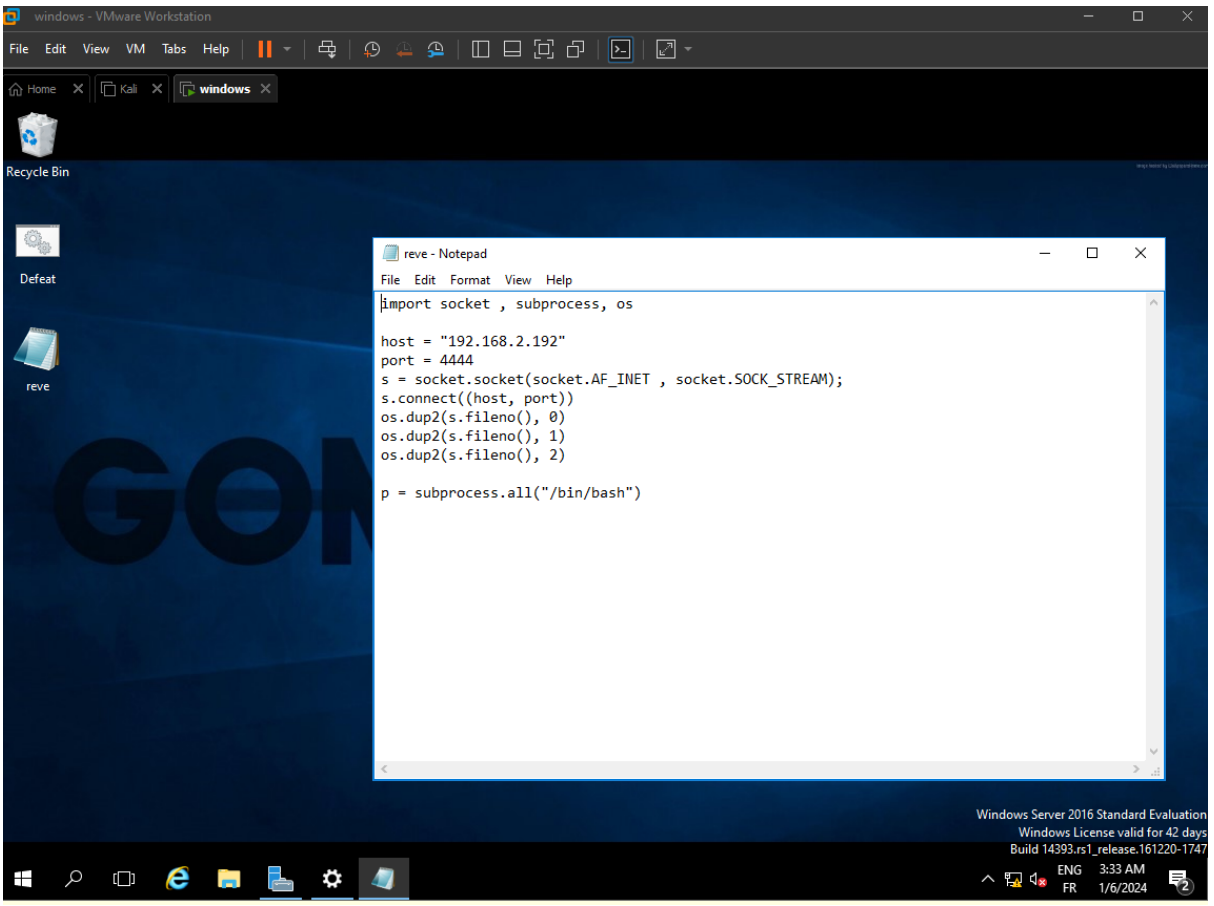
- copy the second file Defeat.bat inside the windows server
- what do you think ? does this file looks suspicious ?
- try to analyse it with windows defender



- **Why the second folder wasn't detected by the Anti-Virus implemented on windows ?**

(Correct answer the file isn't 100% malicious code, it just downloads and launch a malicious file on the system that's why it's not detected Such codes are called Droppers)

- **Open the rev.py file**
- **Which language is this file written in? (correct answer: python)**
- **This file is obfuscated using base64 Decode it https://i.imgur.com/1N5R7St.png**



- **Explain what the code is doing:**
  - **The code sets up a connection to a remote IP address and port.**
  - **It redirects the standard input, output, and error streams to the network socket.**
  - **It opens a new subprocess running a bash shell, effectively creating a reverse shell.**
- **What is the IP of the hacker?**
  - **The IP address of the hacker is specified in the `host` variable, which is set to "192.168.2.192".**
- **On which port is the communication going to be established?**
  - **The communication is established on port 4444, as specified in the `port` variable.**
- **How can we detect such an attack?**
  - **Detecting such an attack involves monitoring network traffic and system logs for suspicious activities. Network Intrusion Detection Systems (NIDS) and Intrusion Prevention Systems (IPS) can be configured to identify unusual patterns or known signatures associated with reverse shells.**
  - **Regularly reviewing system logs for unusual processes, unexpected network connections, or unauthorized access attempts can also help in detecting such attacks.**

- **Firewalls and network segmentation can be used to limit unauthorized outgoing connections.**