

**CSCI-6646-02 Intro to Computer Security**

**Wargame**

**Blue team**

**Incident response**

**Background:**

Defensive security experts on blue teams oversee keeping internal network defences up to date against all cyberattacks and threats. In this wargame lab, your role consists of defending a Windows 7 in your network. Assuming you downloaded malware and installed it by accident, you will identify and contain the threat by using the following instructions.

Instructions:

Please watch this video and install the tool to detect the meterpreter session: <https://www.youtube.com/watch?v=cuLtLBdXKhM>

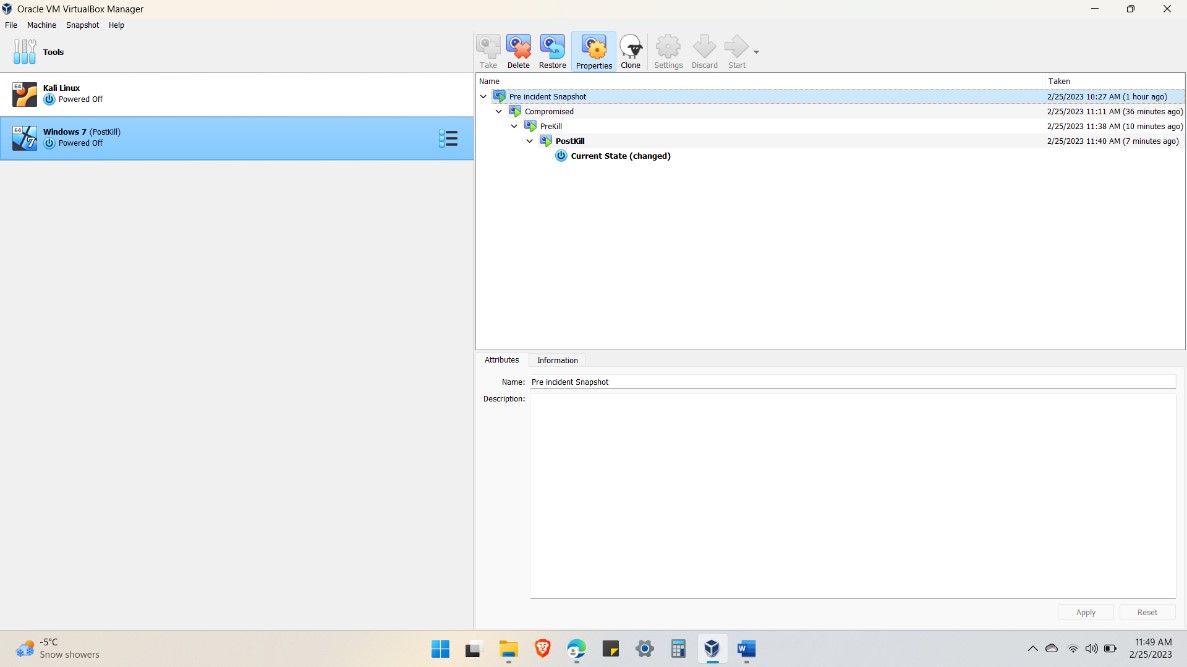
Note: Only download the tool *pwny* in your Windows 7 virtual machine:

Link for the download or *Pwny*: <https://github.com/rvazarkar/antipwny>

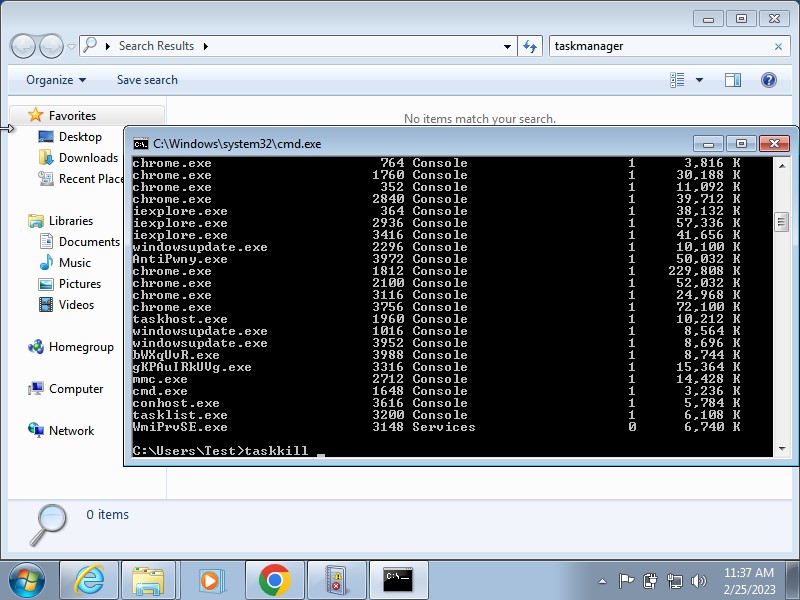
\*\*\*\*\*identification\*\*\*\*\*

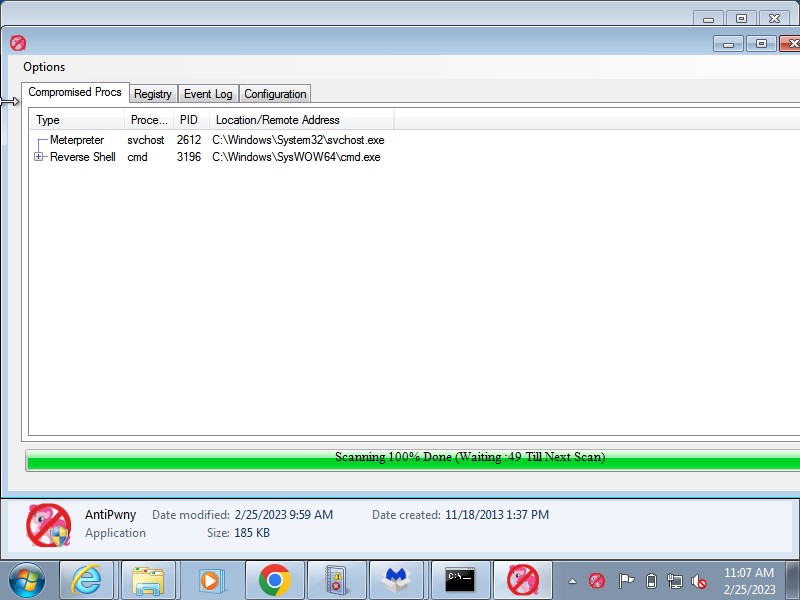
Start by firing up the virtual box and Windows 7. Ensure the virtual box has a bridged connection. Boot Windows 7 has an internet connection. \*\*\*\*Backup\*\*\*\*

* Ensure you save a Windows 7 snapshot for backup and call it a " pre-incident snapshot”.



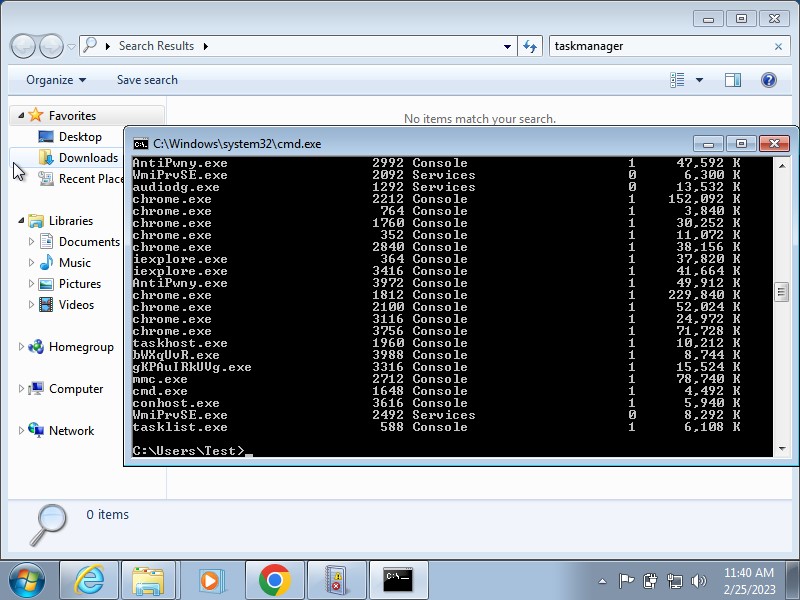
* Find the event logs by typing *event viewer* in the search bar.
* find the malicious process in task manager or in cmd by typing *tasklist.*

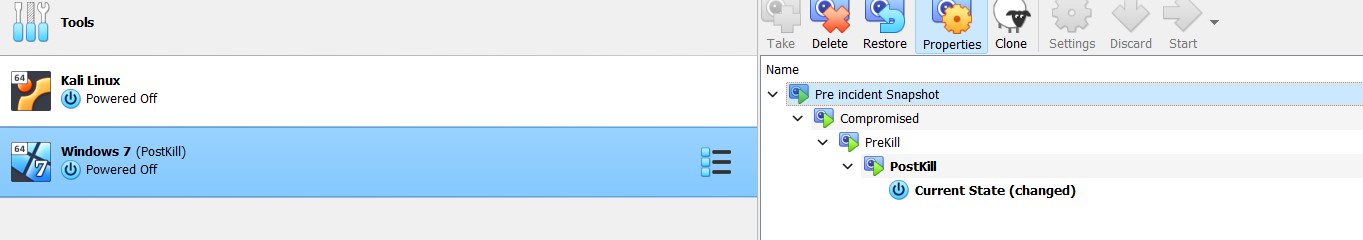


*Use Pwny to find the meterpreter session* 

\*\*\*\*\*\*containement\*\*\*\*\*\*

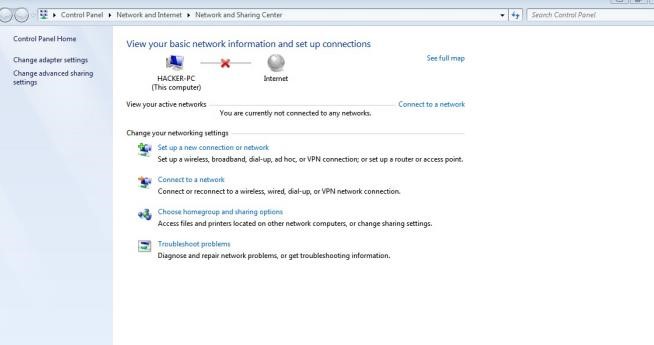
* Kill the malicious process with its PID
* *taskkill /PID /F (ensure you copy and paste the command and just add the PID # as it is case sensitive)*



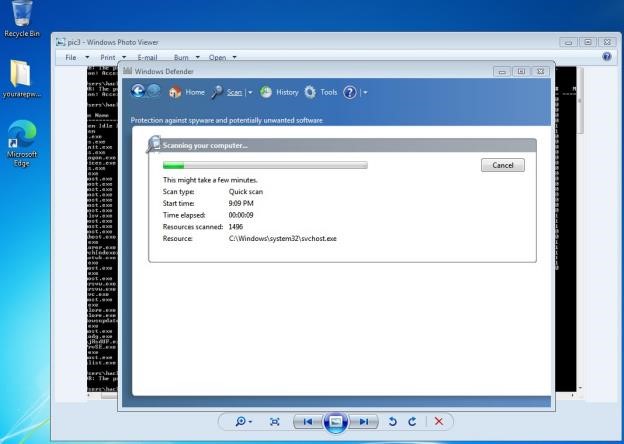


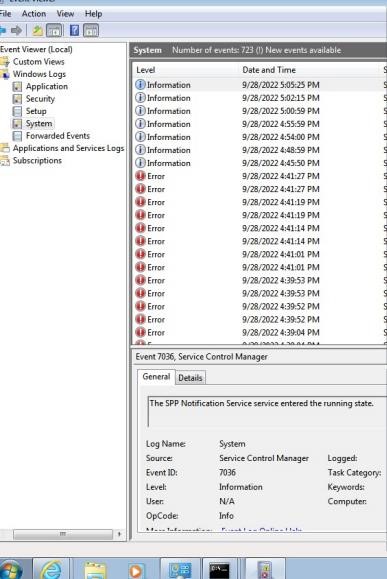
* In CMD, open netstat -aon and find the malicious port and kill the port as instructed in class.

*Netstat -aon*

Completely isolate the windows 7 machine by disconnecting the windows 7 ONLY from the internet. 

\*\*\*\*\*\*eradication\*\*\*\*\*\*

Download Malwarebytes to eradicate the victim's Windows 7 machine and quarantine the malware you downloaded.

* Determine what the attack vector was. (how the attack originated)
* In our case by running the unknown software (windowsupdate.exe) allowed a remote connection to the hacker.
* Find out if the logs (Application, System, and Security logs) have been deleted - snapshots by typing event viewer in the search bar.

\*\*\*\*\*Recovery\*\*\*\*\*

* Restore the snapshots you took at the very beginning
* The outcome of this hacking session is that we should never run malicious software which are downloaded from the public internet.

\*\*\*\*end of the Blue team defensive session\*\*\*\*