Syracuse University

IST-623 Lab#1

Identifying and Removing Malware on a Windows Systems

ThulasiRam RuppaKrishnan

IST 623

Professor Joon Park

Contents

Lab Environment

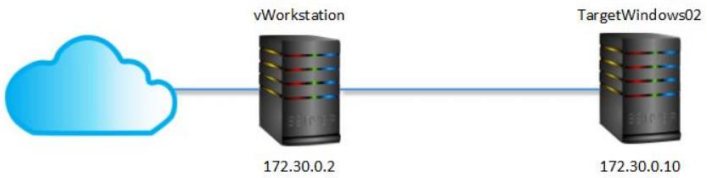
Identifying and Removing Malware on a Windows System

Hacker Techniques, Tools, and Incident Handling - Lab 6

Current Step	Not Started
Progress	0%
StateSave Slot	New

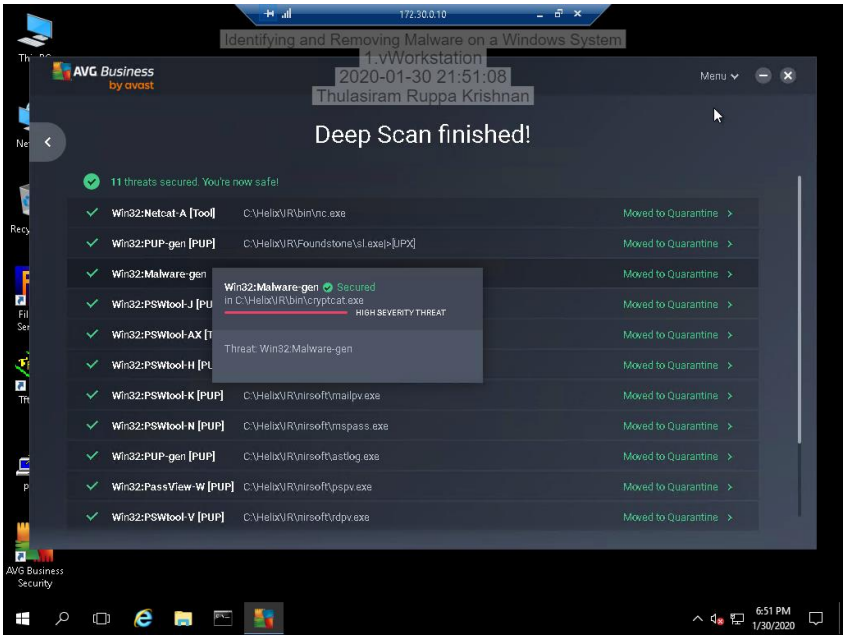
START LAB PREVIEW LAB GUIDE

Topology

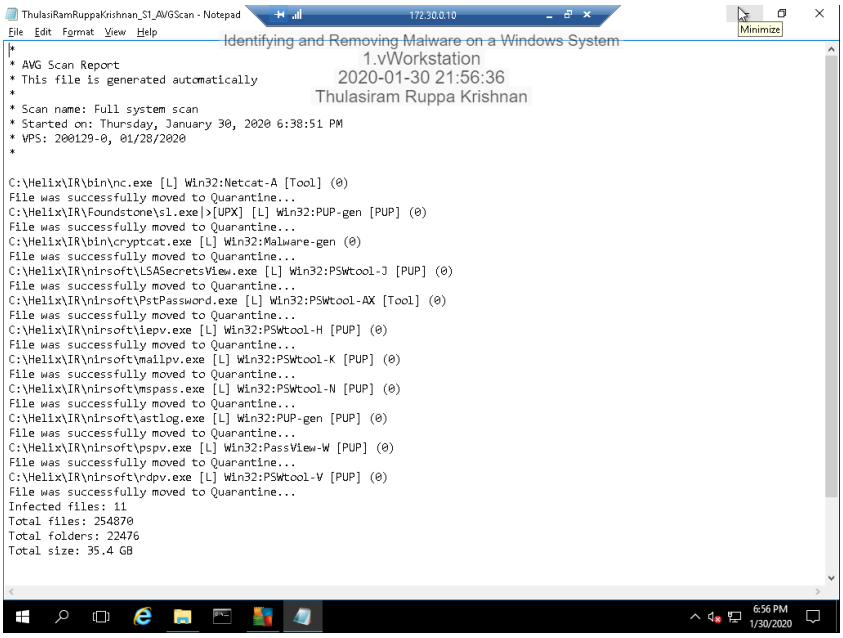


Part 1: Using Antivirus Software to Scan the Potentially Infected System

Scan Summary page showing threat details identified by AVG antivirus is given below

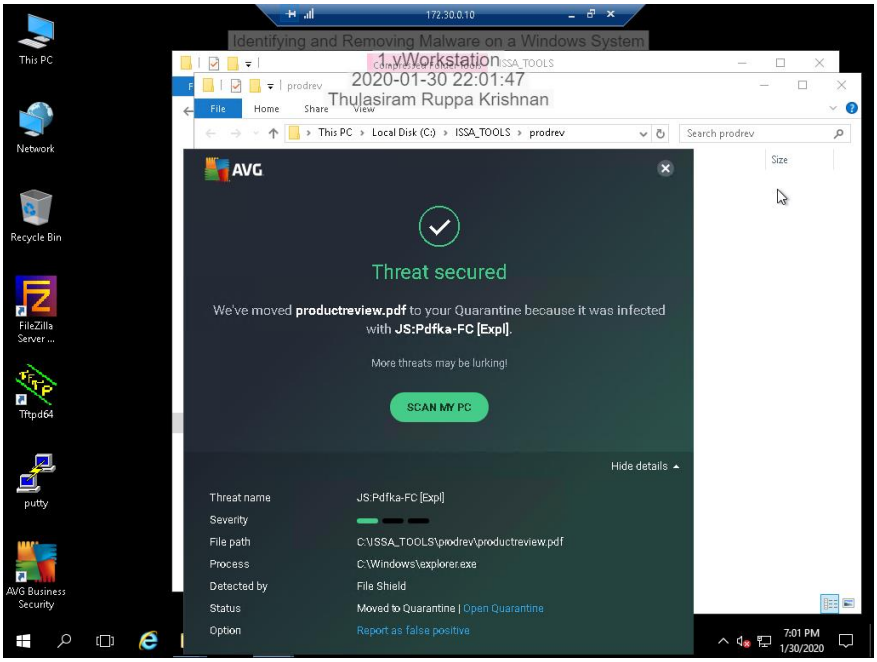


Screenshot of lab report file generated by AVG antivirus scan results are shown below

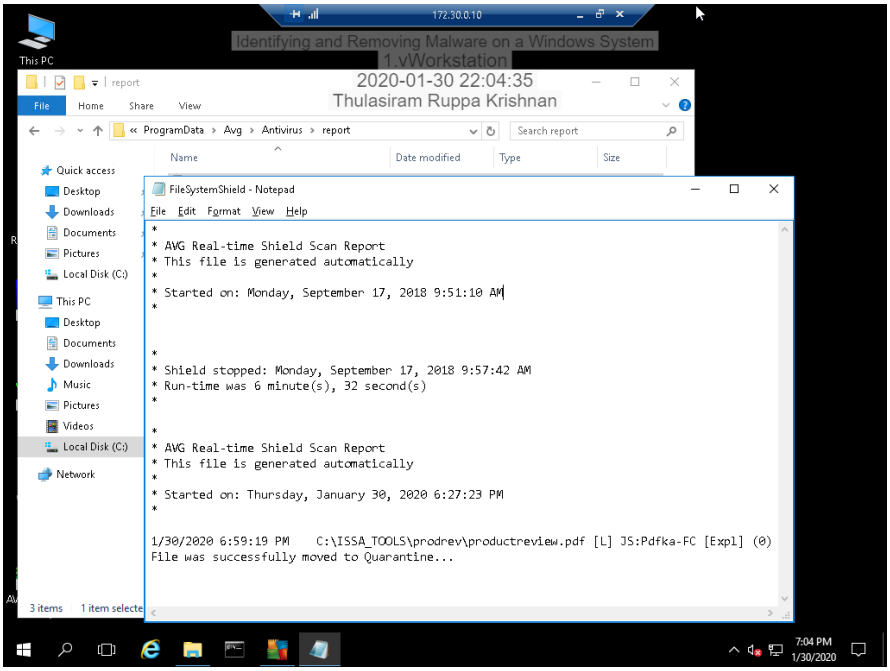


Part 2: Identify Threats in Encrypted Archive Files

Screen capture showing the **Pdfka-FC threat detection**

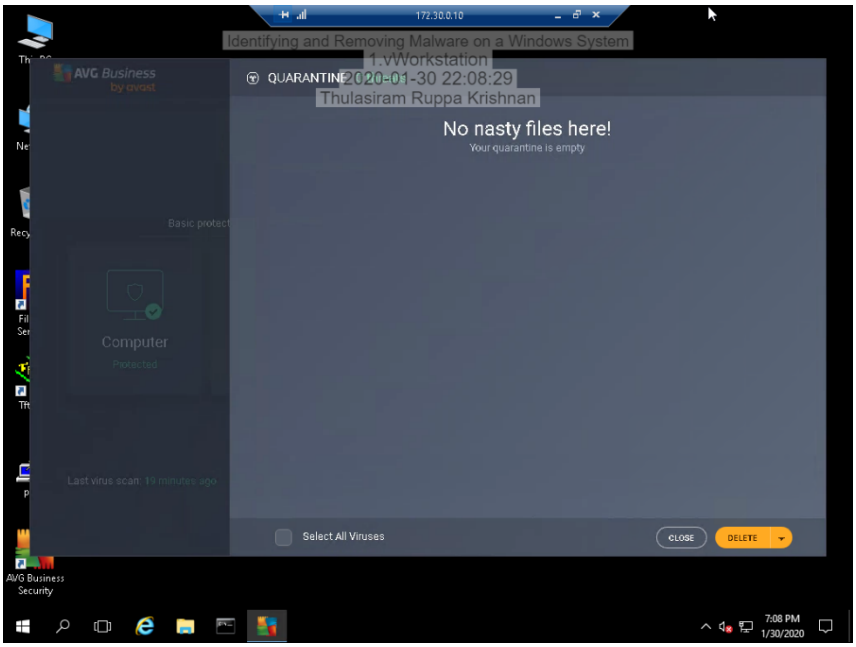


Lab Report file showing Pdfka-FC threat detection in the FileSystemShield file

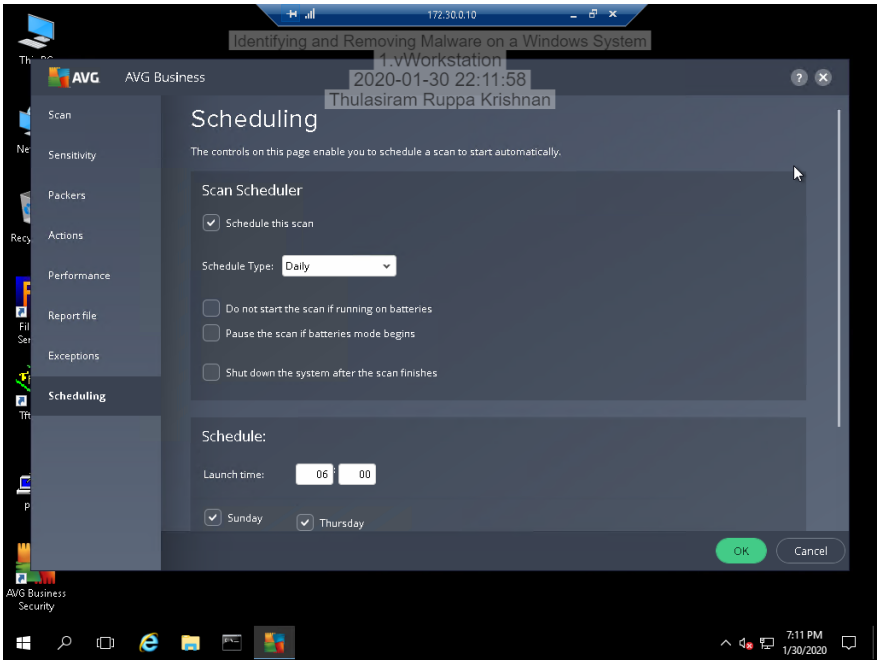


Part 3: Manage AVG Scans and the Virus Vault

Screen capture showing the **empty Quarantine area (Virus Vault)**

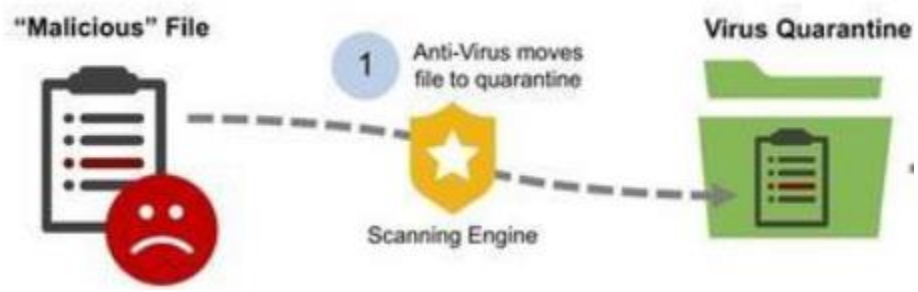


Screen capture showing the **scheduled scan**



Part 4: Working of Quarantine mechanism in antivirus software packages

A quarantine is the process of isolating a file that's suspected of being infected with a virus in order to prevent it from contaminating other parts of your computer.



When an antivirus places an infected file in quarantine, it deletes the file from its original location and makes changes to it so that it cannot run as a program. It then transfers it to a hidden folder that other programs (or yourself as the user) cannot access where it stays until you choose to deal with it. A suspicious file can also be quarantined manually in the rare case that it's not picked up by your antivirus scan. Quarantined files are not deleted unless you want them to be. As mentioned above, quarantining a suspicious file merely relocates the infected file into a safe space on your computer. we need to instruct antivirus to delete the file or otherwise delete it ourselves manually. we can keep a file in quarantine indefinitely, but if an important file that is infected, you should place it in quarantine and clean it.

While quarantining a virus is safe, there is always the risk of your antivirus making a false alert and quarantining a system file that your computer needs to run effectively. Which is why the deleting process is usually left to discretion. Also, we can 'clean' any quarantined files needed, and place them back into their original location.

References

https://www.safetydetectives.com/blog/how-does-antivirus-quarantine-work/