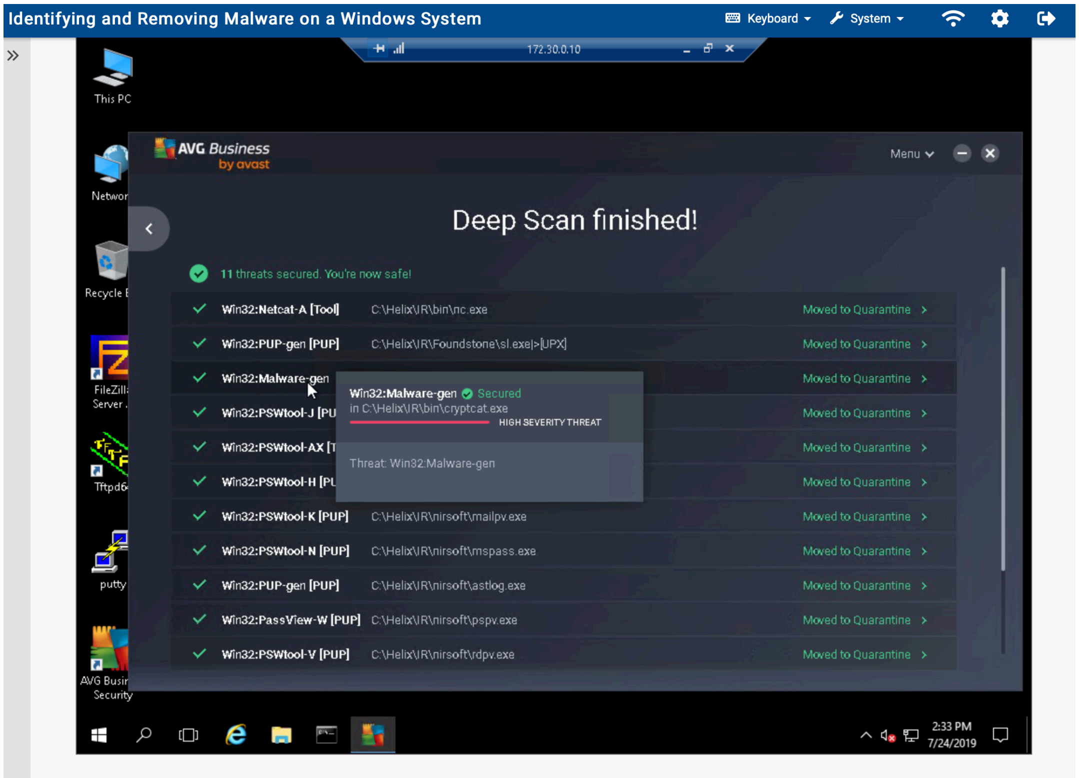
Lab #1: Identifying and Removing Malware on a Windows System

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

Steps #17



Deep Scan finished!

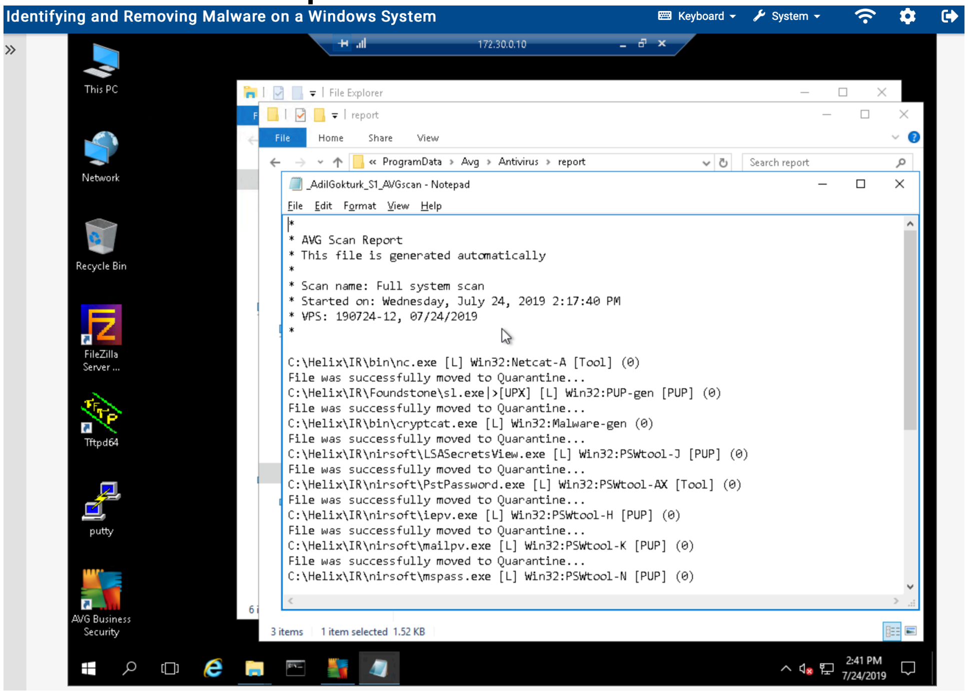
11 threats secured. You're now safe!

✓ Win32:Netcat-A [Tool]	C:\Helix\IR\bin\nc.exe	Moved to Quarantine ›
✓ Win32:PUP-gen [PUP]	C:\Helix\IR\Foundstone\sl.exe|>[UPX]	Moved to Quarantine ›
✓ Win32:Malware-gen		Moved to Quarantine ›
✓ Win32:PSWtool-J [PU		Moved to Quarantine ›
✓ Win32:PSWtool-AX [T		Moved to Quarantine ›
✓ Win32:PSWtool-H [PU		Moved to Quarantine ›
✓ Win32:PSWtool-K [PUP]	C:\Helix\IR\nirsoft\mailpv.exe	Moved to Quarantine ›
✓ Win32:PSWtool-N [PUP]	C:\Helix\IR\nirsoft\mspass.exe	Moved to Quarantine ›
✓ Win32:PUP-gen [PUP]	C:\Helix\IR\nirsoft\astlog.exe	Moved to Quarantine ›
✓ Win32:PassView-W [PUP]	C:\Helix\IR\nirsoft\pspv.exe	Moved to Quarantine ›
✓ Win32:PSWtool-V [PUP]	C:\Helix\IR\nirsoft\rdpv.exe	Moved to Quarantine ›

Win32:Malware-gen ✓ Secured
in C:\Helix\IR\bin\cryptcat.exe
HIGH SEVERITY THREAT

Threat: Win32:Malware-gen

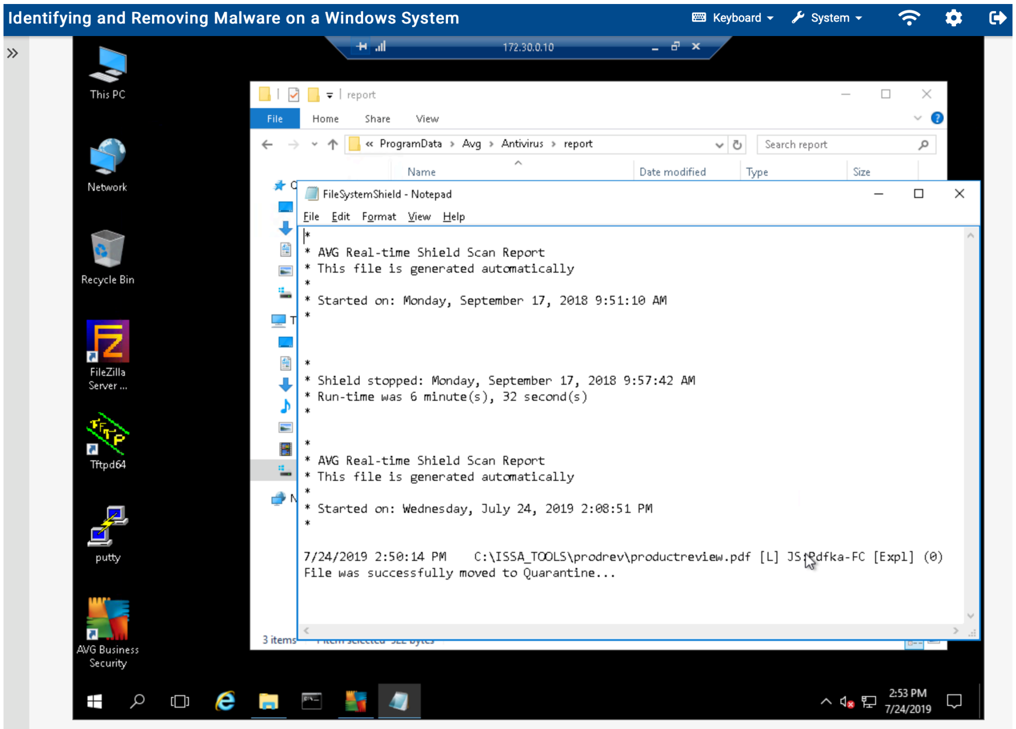
- ## Part 1: Steps #25



```
*
* AVG Scan Report
* This file is generated automatically
*
* Scan name: Full system scan
* Started on: Wednesday, July 24, 2019 2:17:40 PM
* VPS: 190724-12, 07/24/2019
*

C:\Helix\IR\bin\nc.exe [L] Win32:Netcat-A [Tool] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\Foundstone\sl.exe|>[UPX] [L] Win32:PUP-gen [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\bin\cryptcat.exe [L] Win32:Malware-gen (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\LSASecretsView.exe [L] Win32:PSWtool-J [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\PstPassword.exe [L] Win32:PSWtool-AX [Tool] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\iepv.exe [L] Win32:PSWtool-H [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\mailpv.exe [L] Win32:PSWtool-K [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\mspass.exe [L] Win32:PSWtool-N [PUP] (0)
```

Part 2: Identify Threats in Encrypted Archive Files

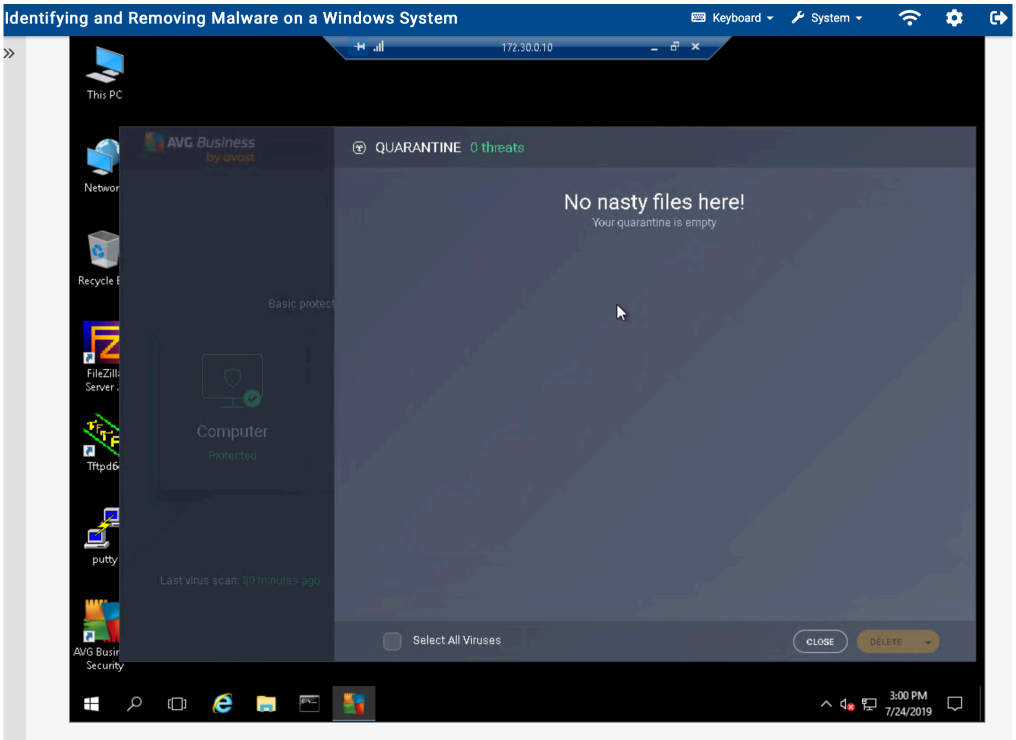
Step #11



```
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Monday, September 17, 2018 9:51:10 AM
*



*
* Shield stopped: Monday, September 17, 2018 9:57:42 AM
* Run-time was 6 minute(s), 32 second(s)
*


*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Wednesday, July 24, 2019 2:08:51 PM
*

7/24/2019 2:50:14 PM    C:\ISSA_TOOLS\prodrev\productreview.pdf [L] JS:Pdfka-FC [Expl] (0)
File was successfully moved to Quarantine...
```

Part 3: Manage AVG Scans and the Virus Vault

Steps #5



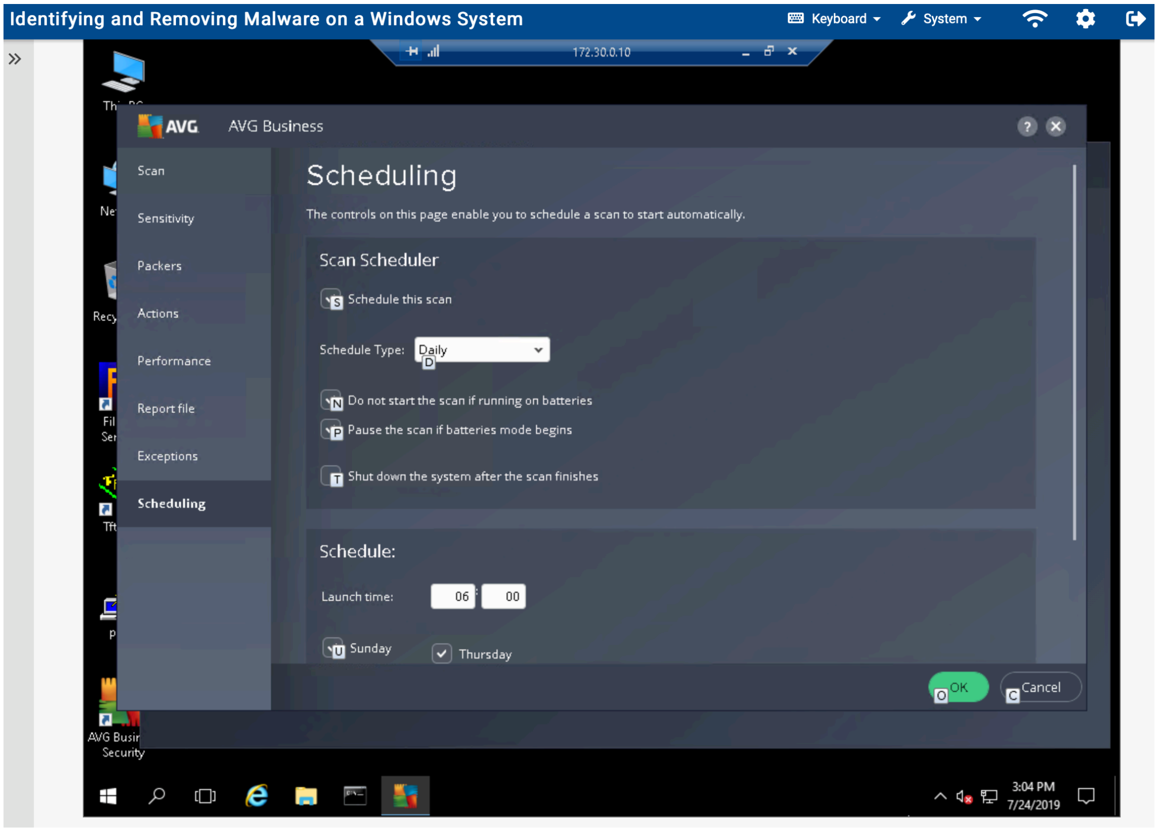
QUARANTINE 0 threats

No nasty files here!

Your quarantine is empty

□ Select All Viruses

Steps #12



Scheduling

The controls on this page enable you to schedule a scan to start automatically.

Scan Scheduler

☑ Schedule this scan

Schedule Type: Daily

☑ Do not start the scan if running on batteries

☑ Pause the scan if batteries mode begins

□ Shut down the system after the scan finishes

Schedule:

Launch time: 06 : 00

☑ Sunday ☑ Thursday

Part 4: Challenge Question
Explain how the Quarantine mechanism is working in antivirus software packages (in 200 words.)

Quarantine is the process of separating a virus-infected file in order to prevent it form t from contaminating other parts of the computer.

When an antivirus program places a virus-infected file in quarantine, it deletes the file form its original location and makes changes to it so that it can't run as a hostile program.

The Antivirus program then transfers it to a hidden folder that other programs or the users cannot access where it stays until the operator choose how to deal with it. A suspicious file can also be quarantined manually in some cases that it's not detected by the antivirus scan.

Quarantined files are not deleted unless the operator wants them to be. Quarantining a suspicious file merely relocates the infected file into a safe space on computer.
The operator/user need to initiate the antivirus program to delete the file or otherwise delete it manually. The operator can keep a file in quarantine

indefinitely, but if an important file that is infected, the operator should place it in quarantine and clean it. While quarantining a virus is safe and the best course of action for infected files, there is always the risk of an antivirus program making a false alert and quarantining a system file that the computer needs to run effectively. Which is why the deleting process is usually left to the operator discretion.