MARYMOUNT UNIVERSITY

Assignment: IT557; Monitoring, Auditing, and Penetration Testing
Assigned: Nov. 18, 2018
Instructor: Professor Ali Bicak
Student Name: George Boakye

LAB REPORT FILE (LAB9)

SECTION 3

Part 1

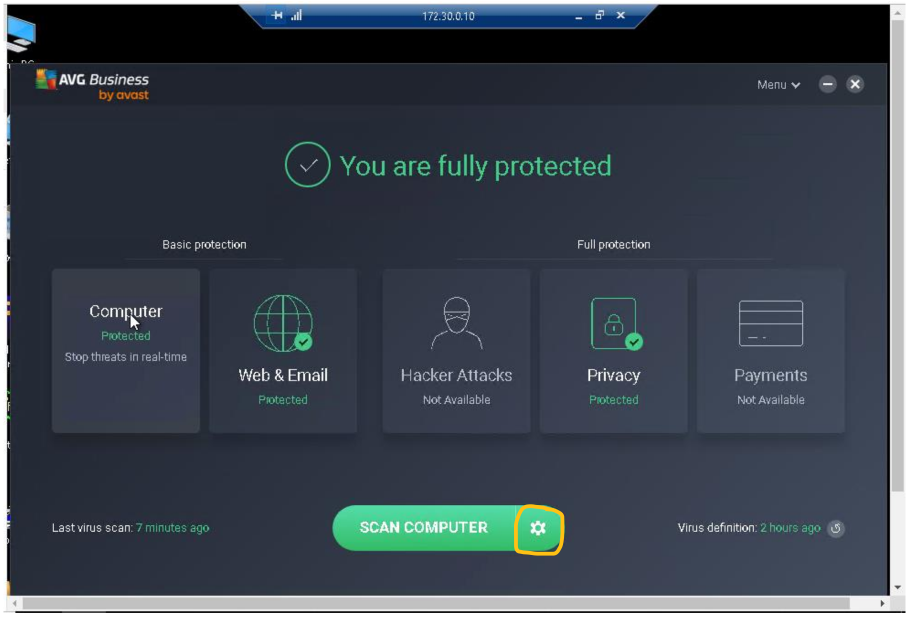
Air-gapping an infected device is far better and secure than connecting to secure antivirus update server when a compromised device has been identified. Infected device must be completely isolated off the network while being cleaned. This is because worms for instance spread by using techniques that are creepy to move from one computer to another through a network. In this sense, a device infection spread from one to another over a network just as vectors of biological infection such as catching cold through sneezing.

This is why it is critical to air-gap devices from a network once a compromise is discovered instead of connecting to secure antivirus update server. There's the high probability when connecting to secure antivirus update server that a threat in question could infect another system in an attempt to removing the threat from the system.

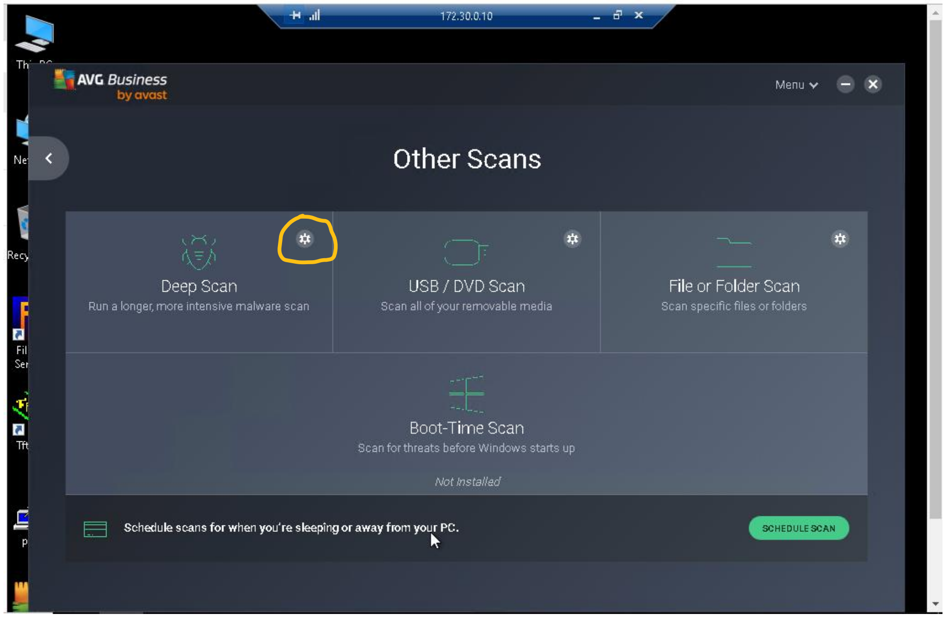
Part 2

Legend: All steps are marked in yellow lines

Click the settings icon next to Scan computer.



Click the configuration button on the top right corner of the Deep Scan section



Other Scans

Deep Scan
Run a longer, more intensive malware scan

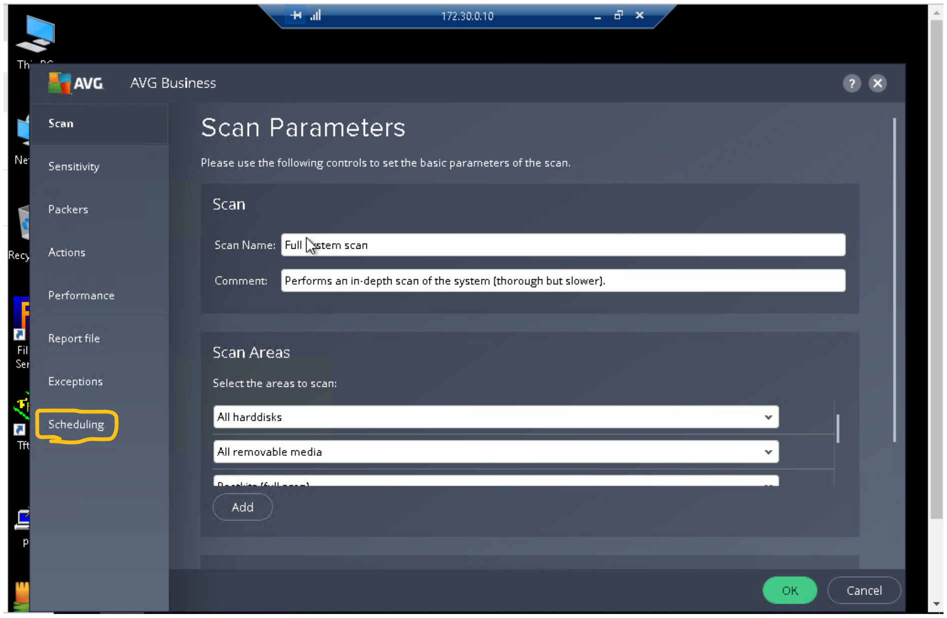
USB / DVD Scan
Scan all of your removable media

File or Folder Scan
Scan specific files or folders

Boot-Time Scan
Scan for threats before Windows starts up
Not Installed

Schedule scans for when you're sleeping or away from your PC.

Click Scheduling at the lower left corner of Scan Parameters window



Scan Parameters

Please use the following controls to set the basic parameters of the scan.

Scan

Scan Name: Full system scan

Comment: Performs an in-depth scan of the system (thorough but slower).

Scan Areas

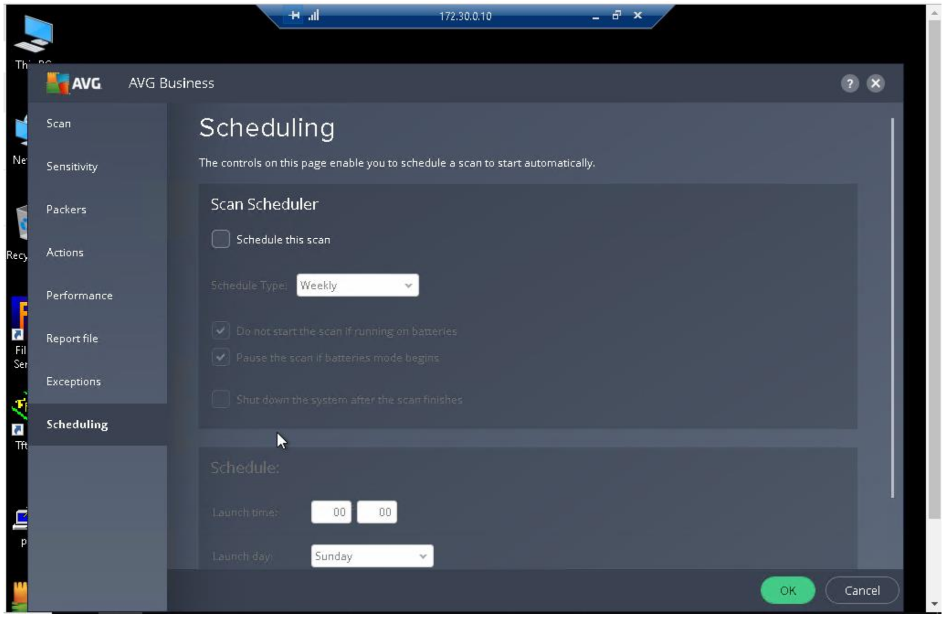
Select the areas to scan:

All harddisks

All removable media

Rootkits (full scan)

In the Scheduling window, check the “Schedule this scan” box



Scheduling

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

Scan Scheduler

□ Schedule this scan

Schedule Type: Weekly

☑ Do not start the scan if running on batteries

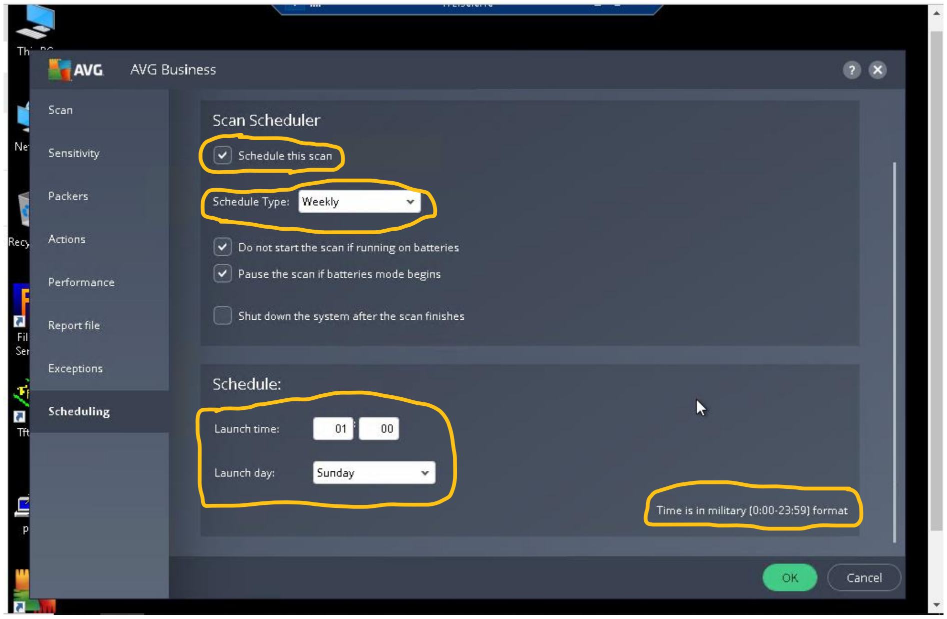
☑ Pause the scan if batteries mode begins

□ Shut down the system after the scan finishes

Schedule:

Launch time: 00 00

Launch day: Sunday



Scan Scheduler

☑ Schedule this scan

Schedule Type: Weekly

☑ 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: 01 00

Launch day: Sunday

Time is in military [0:00-23:59] format

Scroll down to the “Schedule” section
At “Launch time”, type ‘01’ in the first box and ‘00’ which is default in the second box. This is because AVG Business runs the military time format (Lower left corner in the scheduling page)
At “Launch day”, leave it at Sunday which is the default or click the drop-down button to select Sunday if it is not selected by default.
This launch time (01:00) indicates that the schedule is set at 1AM every Sunday as the ‘Schedule type’ is set to weekly.
Click ok when all is set to activate the schedule.

Part 3

Containing a possible outbreak

As an IT Security personnel, Incident Response handler, Operations Security team, or a network administrator, planning a containment strategy or mitigating an imminent danger could be equally as frustrating. Not all threats behave the same and some even update themselves, changing their behavior partway through a disinfection procedure. A number of basic measures have to be taken to isolate and/or clean up the network and devices and to prevent or limit possible reoccurrence.

Measures include:

1. Identifying the reported threat
2. Identifying computers, the threat has compromised
3. Isolating the compromised computers
4. Cleaning the compromised computers, and
5. Prevent reoccurrence

Once the compromised computers have been identified, they must, whenever possible, be taken off the network while being cleaned. If any of the compromised devices is mission-critical and cannot be isolated from the network, depending on the infection, it should be placed in a quarantine networks with some heavily restricted network access. The Security Team must make the necessary preparations and put infrastructure in place to facilitate a successful containment.

In creating the plan, the security team must:

- Assess if any system changes were made on infected computers and how to revert those changes
- Assess when it is safe to add the computers back to the network, and also
- Assess if any threats found can be easily removed by running antivirus scans, or if some additional tasks have to be performed

Even after completing these tasks, the security team must be prepared for the worst and always draft a contingency plan for potential outbreak.

Lessons Learned:

An investment in antimalware software must be made to reduce exposure to threats that are sent into the internal networks by mobile staff.

Educated and awareness training on protecting systems from viruses by running only company authorized Antivirus software should be encouraged.

Client/Network firewalls must also be configured to add an extra layer of security by protecting devices from malicious behavior such as Denial of Service attacks.

Reference

Nahorney, B., & Maengkom, E. (2009). *Containing An Outbreak - How to clean your network after*. Retrieved from Symantec Corporation:

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/security-response-containing-outbreak-09-en.pdf