

Real-World Scenario 2-1: Using Free Malware Scanning Programs

Scenario: As a security administrator, your task is to select a free malware scanning program and scan a computer system.

An anti-malware solution is extremely important when securing a computer's operating system. There are plenty to choose from that will have a price tag attached, but a good security person should also be able to use free tools. Plus, using a free tool provides an easy way to practice without expending any hard-earned capital.

You can select from the following list or search for an alternative using your favorite search engine. These could be programs that are downloadable; if so, be sure that you are downloading the files from a reputable source. There are also online scanners that run directly from within a website. In this case, make sure the website is secured via some kind of website scanning system. Keep in mind that links may change over time, and free software (at the writing of this book) may incur a charge as time goes by.

After you have selected a tool, scan your computer for malware. Remember, this is best done on a test computer if you have one available and not on your main system. Write down the results of your scans.

Windows Defender: (Check first, you might already have this installed on your Windows computer.)

<https://www.microsoft.com/en-us/windows/windows-defender>

Malicious Software Removal Tool:

<https://www.microsoft.com/en-us/download/malicious-software-removal-tool-details.aspx>

Microsoft Safety Scanner:

<https://www.microsoft.com/en-us/wdsi/products/scanner>

Avast:

<https://www.avast.com/index>

AVG:

<https://www.avg.com/en-us/homepage>

Sophos:

<https://home.sophos.com/>

Trend Micro HouseCall:

https://www.trendmicro.com/en_us/forHome/products/housecall.html

Malwarebytes Anti-Malware:

<https://www.malwarebytes.com/>

Spybot Search & Destroy:

<https://www.safer-networking.org/private/>

Real-World Scenario 2-1 Solution

In this example solution we use Windows Defender and a free anti-virus program to analyze two separate computers for viruses. This should be performed on a test computer, but a virtual machine is also acceptable if it doesn't have any direct network connections to the hosting operating system. The steps are as follows:

- Step 1.** Download the appropriate software from the Internet.
- Step 2.** When it finishes downloading, install the program.
- Step 3.** The program should run automatically, but you can also use it to scan your computer for malware. Do so. Click "custom" or a similar option to select different partitions or particular folders. If you find any malware, quarantine it!
- Step 4.** Consider downloading and utilizing other tools in the list to get a firmer understanding of how these types of scanning tools operate.
- Step 5.** When you finish working with the free malware scanning programs, uninstall each of them from the computer and clear the cache on the system. If you want, keep the one that you like the best!

Video Solution: Watch the video solution "2-1: Using Free Malware Scanning Programs."

Simulation: Complete the simulation "2-1: Identifying Malware Types."