

Tutorial 2

Malware

Activity 1 (20mins). Students are required to answer the following questions:

1. What is an antivirus?

- a. A bigger and more dangerous virus.
- b. Software used to duplicate viruses.
- c. Computer software used to prevent, detect and remove malicious software.
- d. A biological agent that reproduces itself inside the cells of living things.

2. Name a type of malware:

- a. Caterpillars
- b. Worms
- c. Lions
- d. Horses

3. A piece of code that can copy itself and damage the system or destroy data.

- a. Computer Virus
- b. Computer Code
- c. Computer Hacker
- d. Computer Worm

4. Which malicious program cannot do anything until actions are taken to activate the file attached by the malware?

- a. Trojan Horse
- b. Worm
- c. Virus
- d. Bots

5. Which method is NOT a sufficient way to prevent malware attacks?

- a. Using and updating legitimate security software and performing daily scans.
- b. Having your firewall on.
- c. Never use an electronic device.

6. Worms can spread and harm independently.

- a. True
- b. False

7. Websites use.... to verify users as human and prevent malicious bot attacks.

Answer:.....

8. Which option below is a sign that suggests the email you received from your bank is possibly forged and an attempt at phishing?

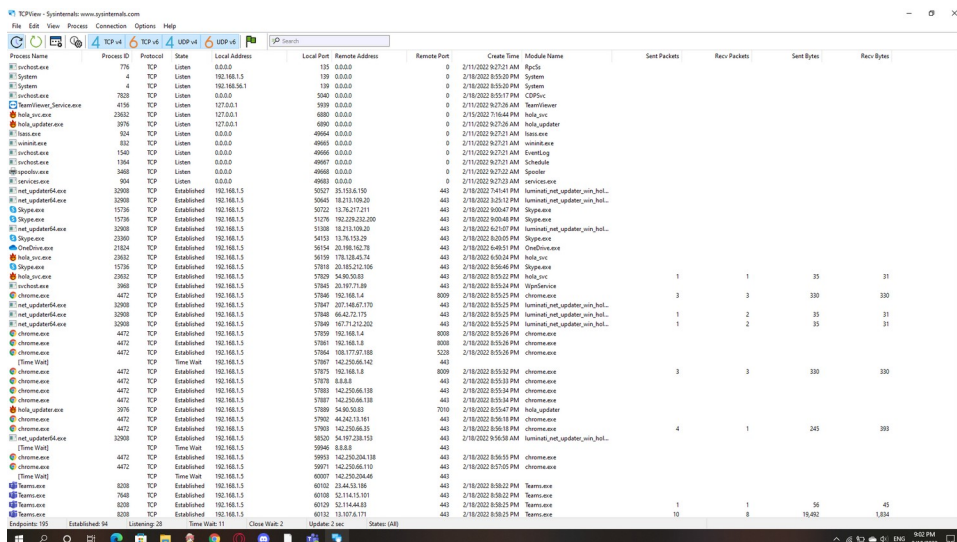
- a. URL of the bank provided in the email
- b. The domain name of the email sender corresponds with the bank name. (e.g. td bank: td@td.com)
- c. The email contains spelling and grammar mistakes.

- Answer:

Students are required to read the **Reading 1** at **Appendix 1**, and try to answer the following questions:

- ### Activity 3 (60 mins)

Instructions can be found in **Appendix 2**.



Appendix 1. Reading 1

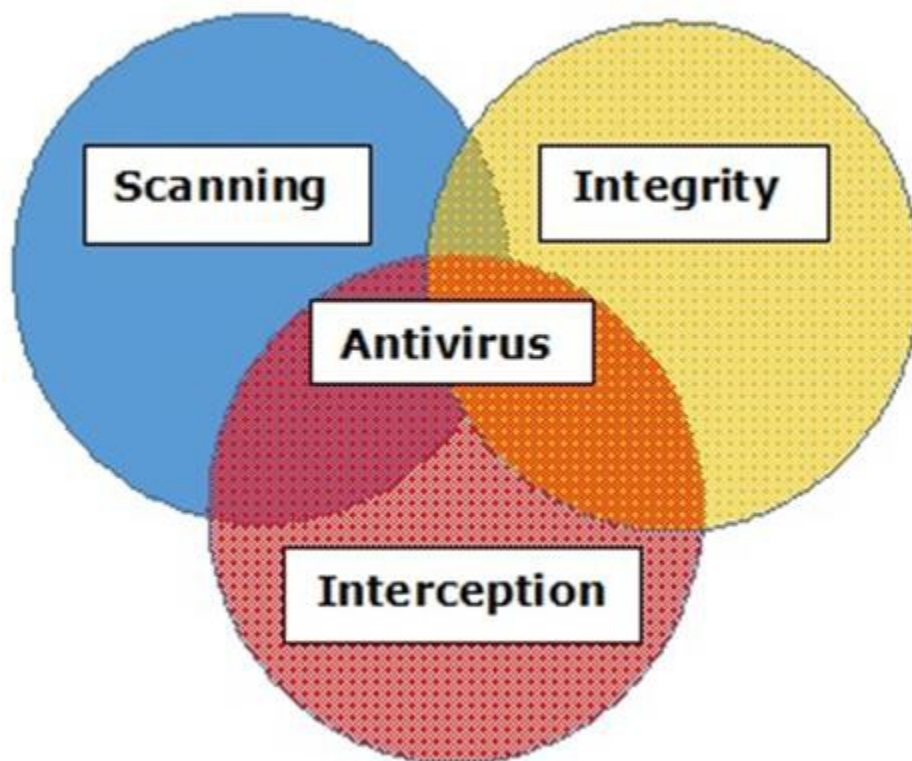
To secure our computers and one of the points was installing and updating antivirus software. Without this software there is a high chance that your systems and networks will be hit and will suffer hacking attacks and also can be affected by the various viruses. It is important that the antivirus scan engine and virus signatures to be updated regularly, we do this because if your system is hit by the latest malware it will be detected.

Basic Functions of Antivirus Engines

All antivirus engines have three components to function accordingly. It is important to have a look at these functions because it will help us for better manual cleaning of viruses in case we need.

- **Scanning** – When a new virus is detected in the cyberspace, antivirus producers start writing programs (updates) that scans for similar signature strings.
- **Integrity Checking** – This method generally checks for manipulated files in OS from the viruses.
- **Interception** – This method is used basically to detect Trojans and it checks the request made by the operating system for network access.

The following image shows the schema for an antivirus engines functionality.



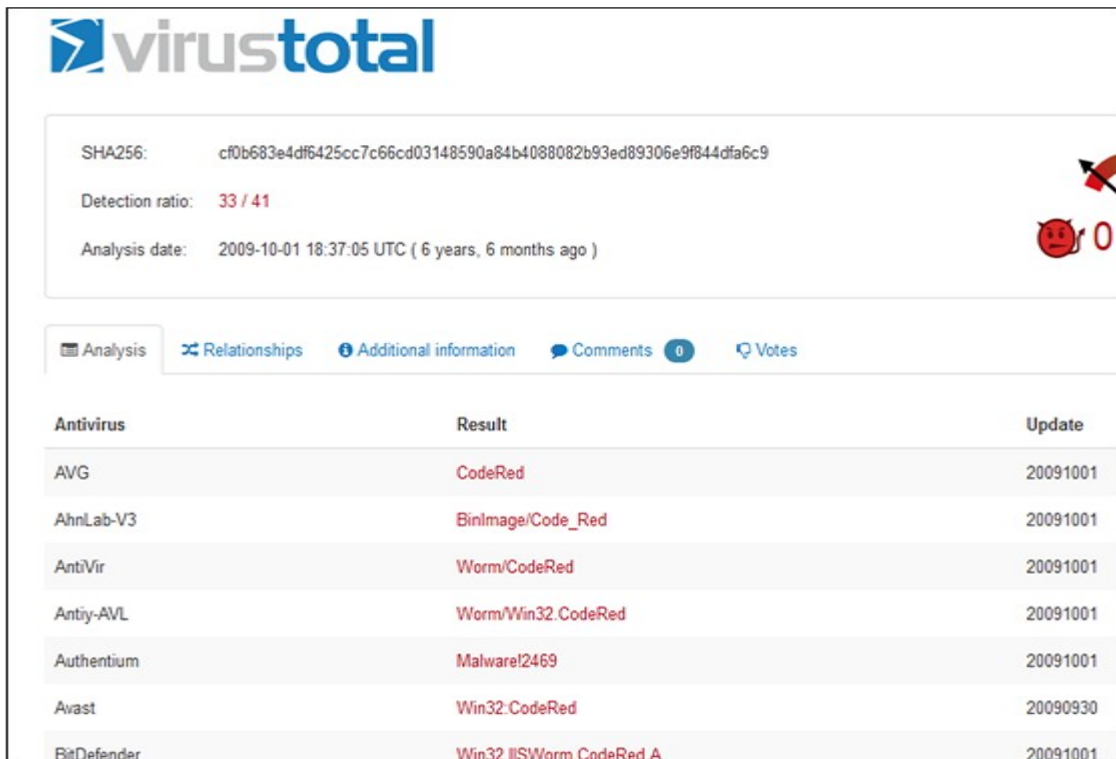
Online Virus Testing

If the system administrator does not have an antivirus installed or suspects a file that is infected. They would recommend to use the online testing antivirus engine which (according to me) is one of the best – <https://virustotal.com/>.

Q. Why this option?

Ans. It is a free and independent service. It uses multiple antivirus engines (41 anti-virus engines), so its result will be showing for all the 41 engines. It updates the engines in real-time.

For further clarity, please see the following screenshot, wherein I uploaded a file with virus and the result is **33/41 (Detection Ratio)**, which means that it has virus and did not pass the class, so it should not be opened.



SHA256: cf0b683e4df6425cc7c66cd03148590a84b4088082b93ed89306e9f844dfa6c9

Detection ratio: 33 / 41

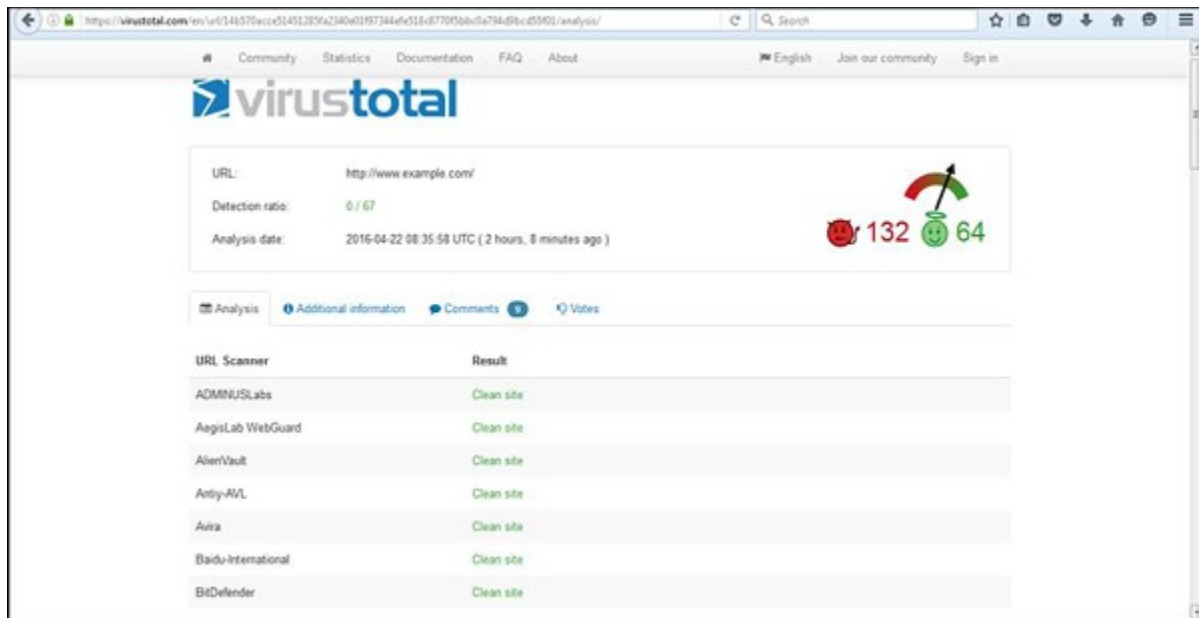
Analysis date: 2009-10-01 18:37:05 UTC (6 years, 6 months ago)

Analysis Relationships Additional information Comments 0 Votes

Antivirus	Result	Update
AVG	CodeRed	20091001
AhnLab-V3	BinImage/Code_Red	20091001
AntiVir	Worm/CodeRed	20091001
Antiy-AVL	Worm/Win32.CodeRed	20091001
Authentium	Malware!2469	20091001
Avast	Win32.CodeRed	20090930
BitDefender	Win32.IISWorm.CodeRed.A	20091001

A good feature of this site is URL checking, before entering to a website you can enter the URL and it checks for you if the site has infection and can harm you.

I did a test with a URL and it came out to be clean and that too 100%, so I can visit it without my computer being infected.



Free Antivirus Software

As this tutorial is hands-on practice, I will show you where to get free antiviruses and where to download in case you don't have enough budget.

The free versions of anti-viruses have nearly identical malware detection scores to the paid versions produced by the same company, but the commercial antivirus makes a small difference in the performance of security and in our case we are system administrators and we want maximum protection in the work environment.

From the PCMagazine (<http://in.pcmag.com/>) you can get a review which are the best top rated free antiviruses at the moment. In the following URL you can check by yourself <http://www.pcmag.com/article2/0,2817,2388652,00.asp>

Let us understand in detail about some of these antivirus software –

Avast Antivirus

This antivirus has good scores in malware blocking and anti-phishing test scans, it can be downloaded from <https://www.avast.com/en-eu/index>

For server installation you need a commercial version.

AVG Antivirus

It can be downloaded from <http://www.avg.com/us-en/free-antivirus-download>. For server installation you need to purchase the commercial version.

Panda Antivirus 2016

It can be downloaded from <http://www.pandasecurity.com/usa/homeusers/downloads/>

It has the following good features –

- Rescue Disk
- USB protection
- Process Monitor

For server installation you will need to purchase the commercial version.

Bitdefender Antivirus

It can be downloaded from <http://www.bitdefender.com/solutions/free.html> A good feature in this antivirus is that it can work entirely in the background. No configuration setting. For server installation you need to buy the commercial version.

Microsoft Security Essentials

Even though it is not among the top-most free antiviruses owing to the Microsoft brand, it is worth a mention that Microsoft itself offers you a free antivirus which is called as Microsoft Security Essentials.

It can be downloaded from <http://windows.microsoft.com/en-us/windows/security-essentials-download>

Commercial Antivirus

I should mention that all the producers of free antiviruses offers their commercial versions too. Based on PC magazine, the best commercial antiviruses are –

- Kaspersky Anti-Virus
- Bitdefender Antivirus Plus 2016
- McAfee AntiVirus Plus (2016)
- Webroot SecureAnywhere Antivirus (2015)

Please see the following link to check by yourself
– <http://www.pcmag.com/article2/0,2817,2372364,00.asp>

MALWARE

Previously, we treated antiviruses which helped us to protect our systems but in this chapter we will treat malwares, how to detect them manually, what are their forms, what are their file extensions, signs of an infected computer, etc. They are important to be treated because the infection rates of businesses and personal computers are too high in nowadays.

They are self-replication programs that reproduce their own codes by attaching themselves to other executable codes. They operate without the permissions or knowledge of the computer users. Viruses or malwares like in real-life, in computers they contaminate other healthy files.

However, we should remember that viruses infect outside machines only with the assistance of a computer user only. These can happen by clicking a file that comes attached with email from an unknown person, plugging a USB without scanning, opening unsafe URLs for that reason. We as system administrators have to remove the administrator permissions of users in these computers. We categorize malwares in three types –

- Trojans and Rootkits
- Viruses
- Worms

Characteristics of a Virus

Following are a couple of characteristics of any virus that infects our computers.

- They reside in a computer's memory and activates themselves while the program that is attached starts running.

For example – They attach themselves in general to the **explorer.exe** in windows OS because it is the process that is running all the time, so you should be cautious when this process starts to consume too much of your computer capacities.

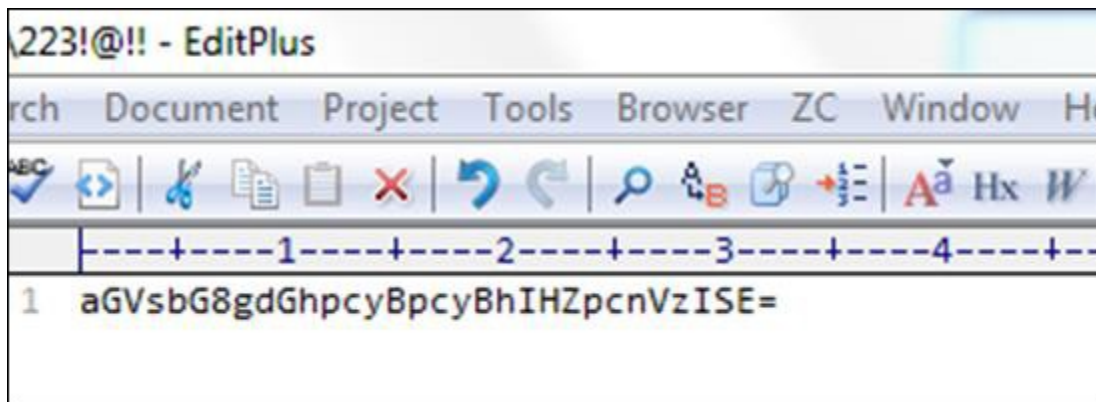
- They modify themselves after the infection phase like they source codes, extensions, new files, etc. so it is harder for an antivirus to detect them.
- They always try to hide themselves in the operating systems in the following ways –
 - Encrypts itself into cryptic symbols, and they decrypt themselves when they replicate or execute.

For example – You can see this in the following image for better understanding as in my computer I found this file.

VC_RED	11/7/2007 8:12 AM	Windows Installer
vcredist	11/7/2007 8:00 AM	Bitmap image
223!@!!	4/23/2016 9:16 PM	File

Modified: 4/23/2016 9:16 PM Date created: 4/23/2016 9:16 PM
 Size: 32 bytes

After finding this file, I opened it with a text editor and as thought the text was not understandable as shown in the following screenshot.



After finding this, I tried it on a base64 decoder and I found that it was a Virus file.



This virus can cause the following to your computer –

- It may delete important data from your computer to gain space for their processes.
- It may avoid detection by redirection of disk data.

- It may perform tasks by triggering an event with itself. For example, this happens when in an infected computer pop-up tables etc., show up automatically on the screen.
- They are common in Windows and Mac OS because these operation systems do not have multiple file permissions and are more spread out.

Working Process of Malwares and how to Clean it

Malwares attach themselves to programs and transmit to other programs by making use of some events, they need these events to happen because they cannot –

- Start by themselves
- Transmit themselves by using non-executable files
- Infect other networks or computer

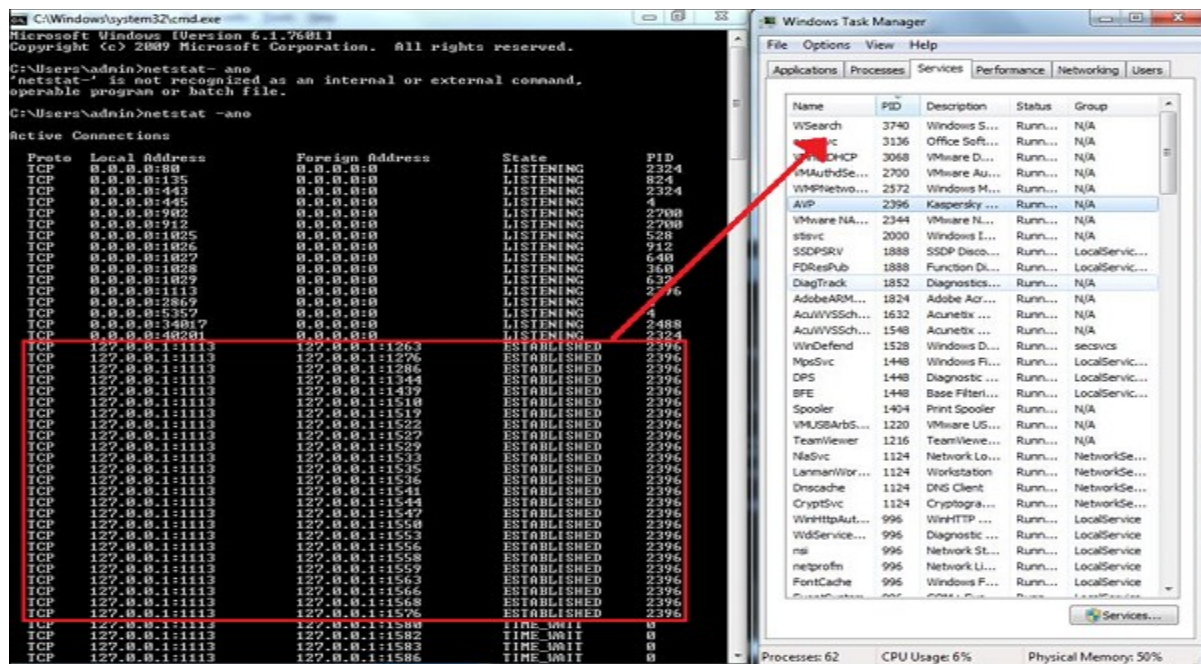
From the above conclusions, we should know that when some unusual processes or services are run by themselves we should further investigate their relations with a possible virus. The investigation process is as follows –

To investigate these processes, start with the use of the following tools –

- fport.exe
- pslist.exe
- handle.exe
- netstat.exe

The **Listdll.exe** shows all the **dll files** being used, while the **netstat.exe** with its variables shows all the processes that are being run with their respective ports.

You can see the following example on how I mapped the process of Kaspersky antivirus which I used along with the command **netstat-ano** to see the process numbers and task manager to see to which process belongs to this number.



Then we should look for any **modified, replaced or deleted files** and the **shared libraries** should also be checked. They generally infect executable program files with extension like **.EXE, .DRV, .SYS, .COM, .BIN**. Malwares changes extension of genuine files, for example: File.TXT to File.TXT.VBS.

If you are a system administrator of a webserver, then you should be aware of another form of malware which is called as **webshell**. It generally is in a .php extension but with strange file names and in an encrypted form. You should delete them in case you detect them.

After that is done, we should update the antivirus program and rescan the computer again.

Detecting a Computer Error from a Virus Infection

In this section we will treat how to detect a computer or OS fault from a virus because sometimes people and system administrators mix the symptoms.

The following events are most likely not caused by a malware –

- Error while the system is booting in bios stage, like Bios's battery cell display, timer error display.
- Hardware errors, like beeps RAM burn, HDD, etc.
- If a document fails to start normally like a corrupted file, but the other files can be opened accordingly.
- Keyboard or mouse doesn't answer to your commands, you have to check the plug-ins.

- Monitor switching on and off too often, like blinking or vibrating, this is a hardware fault.

On the other hand, if you have the following signs in your system, you should check for malware.

- Your computer shows a pop-up or error tables.
- Freezes frequently.
- It slows down when a program or process starts.
- Third parties complain that they are receiving invitation in social media or via email by you.
- Files extensions changes appear or files are added to your system without your consent.
- Internet Explorer freezes too often even though your internet speed is very good.
- Your hard disk is accessed most of the time as you can see from the LED light on your computer case.
- OS files are either corrupted or missing.
- If your computer is consuming too much bandwidth or network resources this is the case of a computer worm.
- Hard disk space is occupied all the time, even when you are not taking any action, for example installing a new program.
- Files and program sizes changes comparing to its original version.

Some Practical Recommendations to Avoid Viruses –

- Don't open any email attachment coming from unknown people or from known people that contain suspicious text.
- Don't accept invitation from unknown people on social media.
- Don't open URL sent by unknown people or known people that are in any weird form.

Virus Information

If you have found a virus but you want to investigate further regarding its function. I would recommend you to have a look at these virus databases, which are offered generally by antivirus vendors.

- **Kaspersky Virus Database** – (http://www.kaspersky.com/viruswatchlite?hour_offset=-1)
- **F-Secure** – (https://www.f-secure.com/en/web/labs_global/threat-descriptions)
- **Symantec – Virus Encyclopedia** – (https://www.symantec.com/security_response/landing/azlisting.jsp)

Appendix 2. Finding Malware

In this exercise, you look at some common ways to find malicious code, malware or tools on a computer system:

1. Unless you already have a Trojan installed on your computer, which is not a good thing, you need something to find.

2. Open a new command prompt **cmd** and type **netstat -an**. You should see a listing similar to the one shown here:

```
C:\>netstat -an
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1027 0.0.0.0:0 LISTENING
TCP 0.0.0.0:12345 0.0.0.0:0 LISTENING
```

Your results should indicate that port 80 is listening. Did you notice anything else unusual in your listing? Did you notice anything unusual in the listing shown here?.

3. In your browser, go to

<https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview> and download TCPView. This free GUIbased process viewer shows you information on running processes in greater detail than netstat. It provides information on all TCP and UDP endpoints on your system, including the local and remote addresses and the state of TCP connections.

4. Close TCPView and go to

<https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>

From there, you can download another process viewer tool called Process Viewer. You will find that it is similar to TCPView.

5. Finally, review a Trojan-removal tool called MooSoft's The Cleaner. This is a system of programs designed to keep your computer and data safe from Trojans, worms, keyloggers, and spyware. It can be downloaded from <http://en.kioskea.net/download/download-16047-moosoft-s-the-cleaner>.

After installation, let the program run to see whether it flags Netcat or any other files. Afterward, you can remove Netcat or any of the other programs installed during this exercise.