CS336 Homework Assignment #5

Due: Friday Nov 5th, 2021, 5:00pm on BbLearn
Turn in: Detailed answers to the questions below
Points: 70 points

(10 points) 1. Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

(10 points) 2. Suppose that while trying to access a collection of short videos on some website, you see a pop-up window stating that you need to install this custom code in order to view the videos. What threat might this pose to your computer system if you approve this installation request?

(10 points) 3. Suppose you observe that your home PC is responding very slowly to information requests from the net. And then you further observe that your network gateway shows high levels of network activity, even though you have closed your email client, web browser, and other programs that access the net. What types of malware could cause these symptoms? Discuss how the malware might have gained access to your system. What steps can you take to check whether this has occurred? If you do identify malware on your PC, how can you restore it to safe operation?

(10 points) 4. Why is logging important? What are its limitations as a security control? What are pros and cons of remote logging? Consider an automated audit log analysis tool. Can you propose some rules which could be used to distinguish "suspicious activities" from normal user behavior on a system for some organization?

(10 points) 5. What are the advantages and disadvantages of using a file integrity checking tool. This is a program which notifies the administrator of any changes to files, on a regular basis? Consider issues such as which files you really only want to change rarely, which files may change more often and which change often. Discuss how this influences the configuration of the tool, especially as to which parts of the file system are scanned, and how much work monitoring its responses imposes on the administrator.

(10 points) 6. Some have argued that Unix/Linux systems reuse a small number of security features in many contexts across the system, while Windows systems provide a much larger number of more specifically targeted security features used in the appropriate contexts. This may be seen as a trade-off between simplicity and lack of flexibility in the Unix/Linux approach, against a better targeted but more complex and harder to correctly configure approach in Windows. Discuss this trade-off as it impacts on the security of these respective systems, and the load placed on administrators in managing their security.

(10 points) 7. A flaw in the protection system of many operating systems is argument passing. Often a common shared stack is used by all nested routines for arguments as well as for the remainder of the context of each calling process.
(a) Explain what vulnerabilities this flaw presents.
(b) Explain how the flaw can be controlled. The shared stack is still to be used for passing arguments and storing context.