CS336 Homework #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?

- The USB could have any number of malware programs on it. Plugging in the USB stick could give an outside attacker an inside machine they can exploit to access other machines on the network.

What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

- The most obvious thing would be: don't try to figure it out yourself, just give it to the IT department, or to lost and found. Other than that, maybe you could check it out on an isolated system, like a live USB of Linux on a PC that doesn't have any important information, to check it out where it can't do any harm, in case it does in fact it have malicious content.

(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?

- The code would probably be in the form of a browser extension. To do the things this extension wants to do, it will probably request the ability to read and modify web pages you view. This could give it access to virtually everything you do in your browser, maybe even login info. It could also potentially serve as an access point for other malware to be installed.

(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?

- This could be some sort of DoS attack, but it is more likely some sort of bot malware that is using your system's resources for some other purpose. This could be through some browser extension that was installed, or software downloaded from an untrustworthy source. If you do identify the malware, it may be as easy as uninstalling a program or running a malware removal tool, or if it's a more resilient virus it may take reinstalling software or the OS.

(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?

- Logging is useful in that it lets you track who does what, so that if someone is trying to do something they shouldn’t, you can see it happening and hold them accountable.
- Logging is useful only so far as the log is protected from being altered. If the attacker can hide the fact that they’ve done something, the log becomes useless.
- I’m a little unsure what remote logging is, I assume it is a log that is kept on a different machine than the one which is having its activities logged. This would be useful as long as that machine is secure, and the network between the machines is also secure, so the log cannot be modified on the way to the remote system.
- Rules: Maybe keep track of what files different types of users should be normally accessing, and flag when they access something out of the ordinary. Also, maybe log connections to other computers/servers, if a connection is made to a device other than a list of approved ones, check it out.

(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.

- Advantages:
    - Being able to tell when files have been changed will be useful in ensuring important files are only modified when they should be. This is especially useful for files that should not change often.
- Disadvantages:
    - If a file is expected to change often, checking that it has changed won’t mean much.
    - One of the issues would be figuring out a good balance of when to report changes.
- Possible solutions:
    - Some files might get changed dozens of times a day, but not be important changes. They don’t really need to be tracked, so the tool could be set up to only monitor important files that don’t change often, or shouldn’t change at all. This would help keep the administrator from being overwhelmed with endless notifications about trivial changes to files.

(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.

- It sounds like Unix/Linux systems would require less work on the administrator's part to keep secure, as there are fewer systems for them to work with. However, if these systems *do* become compromised, the attacker will have access to much more of the system than they would on Windows.
- For Windows, it seems like the administrator would have a tougher time keeping track of every security module that is running. They may not be able to keep the system as secure, since there are more things to worry about. However, unlike Unix/Linux, if a system is compromised, the ability of the attacker to cause trouble will be limited by the scope of that system.

(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.

a) This flaw results in the vulnerability we saw in one of the labs. An insecure program may be exploited to view or even modify the stack, not just affecting that program, but potentially compromising other programs as well.
b) I did some research on this, one thing I found in Windows is that the OS maintains "shadow stacks" that keep track of the intended flow of the program, so if the program does something strange (like try to launch a root terminal), it will be obvious that something has gone wrong. Another article talks about what the gcc compiler does (or at least did at the time of writing). It pushes a randomly generated value onto the stack directly after the buffer; between it and the return address. Before returning, it checks the value to see if it is the same. To exploit a buffer overflow attack, the attacker will have to write over the value, but they won't know what the value is to keep it the same. So, if the value has been changed, the program will crash, instead of running the malicious return value.