CMPT 479 Assignment 1

Junchen Li

301385486

2022/6/19

1. i. (a). It violated integrity in CIA principles because Crypto-jacking can be done through the background scripts on a webpage, which means it modifies information without authorization.

(b). It violated availability in CIA principles because a potential backdoor means that the system and equipment cannot be guaranteed to work properly. It means that there is no qualified availability.

(c). It violated Confidentiality in CIA principles because this malware accessed the private information of politicians and activists. Under unauthorized condition, information cannot disclose to attackers.

(d). It violated Availability in CIA principles because the Meris botnet will break the MikroTik routers and control it. It will influence the safety of devices and system. So the availability in CIA will be violated.

ii. (a). This malware belongs to Network by method of spread. It can be done through background scripts.

(b). This malware belongs to Planted Malware, since the NSA is sole editor of this algorithm's standard. It installed by people who control the system.

(c). This malware belongs to Trojan, since zero-day vulnerability will send a file that looks like a GIF file and tricking the user into clicking it. It packaged with unharmed file

(d). This malware belongs to Network, since the it will compromise the routers and allow to stall the admin password. It inflection very fast.

iii. (a). The behavior-based scanning will prevent the attract. Users will know what's the CPU really doing and if it is have the correct behavior. Also they can go over the code to check if the background script changed or not.

(b). Code analysis and software testing both are good idea because it has chance to discover the backdoor in the random number generator.

(c). Scanning is a great idea to prevent the attract, it can check if there is a monitor behavior, scanning the memory and program code.

(d). One method is behavior scanning since it will check if admin password has been viewed or not. And software testing for checking if it will steal the admin password or not.

2. (a) T This is correct because C or C++ is known as the underlying language. It can be easier for us to use them to detect system defects. We can keep it simple/stupid. And we can do least common Mechanism, Least Privilege. so we can use C or C++ because of its "work factor".

(b) T It is true, since the least privilege is means subject should give min necessary privileges for task. If this implementation is poor, there will be a lot of privileges could be pass and it is more easy to cause Buffer overflow.

(c) T This is true. The fail-safe defaults mean when failed, there should be no threat to data security and system should revert to secure default. The purpose of stack canaries are to check if the original value is equal to the after-operator value. If is not the same, which means an overflow happened and it will stop. System state maintains to default.

(d) F This is false. The XSS attacks is an injection that malicious scripts are injected into some web page. They do not need to gain full control over the web server first. Attacks are all sent from trusted sources and therefore run under permissions granted to that system

(e) T This is true. Firstly, the Heartbleed is a serious open-source software bug while a format string vulnerability is better than that. Also, the Heartbleed will cause a more serious problem that could endanger lives.

3. i. (a) Due to previous incidents of hackers using vulnerabilities in applications such as Excel to remotely control customer computers. On June 9, 2010 Microsoft released a patch for the latest security update. It released a total of 10 patch packages for 34 system vulnerabilities. Those patches designed for Office software as well as IE browser, etc. Users should download the patches and update their software in time to prevent attacks happened

(b) Before Android API version 4.4, there was a security vulnerability in Google's Webview. The website could be injected by JS and then obtain important information from the client. It was even easy to call native code for illegal operations. After the problem was discovered Google made an emergency change. Defensive measures were added in subsequent versions. Users must update this patch package as soon as possible to ensure that there is no further risk of leakage of important personal information.

(c) First of all, antivirus software cannot follow up with the times. Nowadays, hackers are constantly updating their attacks methods. Anti-virus software cannot have good timeliness. For example, Stealth techniques, can be interrupted to avoid detection or can be disguised as a file mode and hidden in memory. Another example is Rootkits, which can change the behavior of system functions to make them undetectable. It is worth noting that when installing antivirus software there is a possibility contain a Trojan virus of its own. It is also possible that a Trojan virus may have Zip bombs, compiler bombs. So the antivirus software becomes a carrier for the virus. Secondly, when scanning for antivirus, the system will have the behavior of asking for too many permissions. Like Backdoors or Spyware, they will monitor user information in the system by scanning for virus features and use all kinds of permissions generously. So looking at antivirus software from a more professional perspective is not a highly recommended approach. Its functionality, as well as its efficiency, cannot be guaranteed

(d) Changing passwords frequently is better than relying on password management. According to the Saltzer-Schroeder design principles, it violates the Least Common Mechanism, since passwords have common properties, including privacy and the same level of complexity. So the best approach is to reduce the number of users who rely on password management to manage their all passwords. Recording passwords is equivalent to backing up your own information, which has a better Least Common Mechanism. Secondly, it has better Fail-safe defaults; if password management is monitored or compromised, all passwords are lost and all information is not secured. Howeverr, changing passwords frequently can ensure that if you lose your password, you can always change it and keep your information safe. The user is not aware of the intrusion of the password management. Therefore, changing passwords has better Fail-safe defaults, i.e. when an error occurs, the system returns to its initial state.