CMPT 403: Written Assignment 1

Vaibhav Saini – 301386847

Question 1

(a)

i. CIA principle violated: Availability

Explanation: The crypto-jacking incident described in this news story violates the availability principle. By using the victim's computing resources to mine cryptocurrencies, the attacker consumes the victim's CPU power, resulting in reduced availability of computing resources for the victim's own use. While it may be argued that crypto-jacking violates Confidentiality and Integrity as well by stealing and tampering with victims computing resources.

ii. Method of spread: Using webpages to run background scripts

Explanation: The malware in this case spreads through background scripts on a webpage. When a user visits the webpage, the scripts are executed without their knowledge, utilizing their computing resources for crypto mining.

iii. Counter-measure: Implementing security measures such as disabling background scripts

To prevent crypto-jacking attacks, it is important to implement proper security measures. This includes using secure browsing practices, such as regularly updating web browsers and enabling automatic security patches. Employing ad-blockers and anti-malware software can also help detect and block malicious scripts on webpages. Educating users about the risks associated with visiting unfamiliar websites and the importance of avoiding suspicious links can also be an effective countermeasure.

(b)

i. CIA principle violated: Confidentiality

Explanation: The presence of a potential backdoor in the Dual EC DRBG random number generator compromises the confidentiality principle. If the backdoor is exploited by an attacker, it enables them to fully compromise cryptography based on this tool, potentially leading to unauthorized access to confidential information.

ii. Method of spread: Backdoor

Explanation: The presence of a potential backdoor in the Dual EC DRBG random number generator can be exploited with the help of malware like trojan horse where it may use the backdoor to compromise the systems and leak information.

iii. Counter-measure: Switching to different secure and vetted cryptographic algorithms

To prevent potential compromises due to backdoors or vulnerabilities in cryptographic algorithms, it is crucial to use algorithms that have been thoroughly vetted by security experts and have undergone extensive review processes. Switching to widely recognized and trusted algorithms can help mitigate the risk of backdoors. Additionally, maintaining an open and transparent process for the development and review of cryptographic standards is important to ensure their integrity and security.

(c)

i. CIA principle violated: Privacy

Explanation: The use of the Pegasus malware for surveillance on high-profile targets violates the privacy principle. By exploiting a zero-day vulnerability in the Safari Webkit and installing surveillance software on victims' iPhones, attackers gain unauthorized access to private information and conduct surveillance without the knowledge or consent of the targeted individuals.

ii. Method of spread: Social engineering (file deception)

Explanation: Pegasus malware spreads through social engineering techniques. Attackers send a file to the victim that appears to be a harmless GIF file, but when clicked, it installs the surveillance software on the victim's iPhone.

iii. Counter-measure: Regular security updates and vulnerability patching

To protect against the Pegasus malware and similar threats, it is crucial to regularly update software and apply security patches. Software vendors should promptly release updates to address known vulnerabilities, and users should install these updates as soon as they are available.

(d)

i. CIA principle violated: Availability

Explanation: The Meris botnet's activities, including DDoS attacks and demanding ransoms, violate the availability principle. By compromising MikroTik routers and gaining control over them, the botnet operators disrupt the availability of targeted websites by overwhelming them with a large volume of malicious traffic.

ii. Method of spread: Exploiting vulnerability in 3rd party software/hardware

Explanation: The Meris botnet spreads by exploiting a directory traversal vulnerability in MikroTik routers. This vulnerability allows remote attackers to steal the admin password and gain full control over the compromised devices.

iii. Countermeasure: Regular router firmware updates and avoid using default passwords on routers

To prevent the Meris botnet attack and similar router-based attacks, it is essential to regularly update router firmware to patch known vulnerabilities. Additionally, router administrators should follow best practices for secure configuration, such as using strong passwords, disabling unnecessary services, and applying access control lists (ACLs) to limit access to the router's management interface. Network traffic monitoring and employing traffic analysis tools can also help detect and mitigate DDoS attacks in real-time.

Question 2

(a) False, Buffer overflow attacks typically involve overwriting return addresses on the stack. By overflowing a buffer with more data than it can hold, the attacker can overwrite the return address of a function and redirect the program's execution to a malicious code or arbitrary memory location. Overwriting the return address is a common goal of buffer overflow attacks.

(b) True, Minimizing privileges in critical programs can help mitigate buffer overflow attacks. By running critical programs with minimal privileges or in a restricted environment, the potential damage caused by a successful buffer overflow attack can be limited. If an attacker manages to exploit a buffer overflow vulnerability, their access and control will be constrained by the reduced privileges, reducing the impact of the attack.

(c) True, Return-Oriented Programming (ROP) is a technique used in certain advanced exploitation scenarios, particularly when mitigations like stack canaries are present. ROP attacks involve chaining together short sequences of instructions, known as gadgets, from existing code segments in the program. Since ROP attacks utilize existing code instructions instead of injecting new code, they can bypass stack canaries, which are security mechanisms that detect modifications to the stack.

(d) False, XSS (Cross-Site Scripting) attacks do not require the attacker to gain full control over the web server. XSS attacks involve injecting malicious scripts into web pages, which are then executed by the victim's browser. The attacker can achieve this by exploiting vulnerabilities in user input handling or inadequate input sanitization on the website.

(e) False, If there is a format string vulnerability in OpenSSL, it would not necessarily be a more serious bug than Heartbleed. Heartbleed was a critical vulnerability in the OpenSSL library that allowed an attacker to extract sensitive information, such as private keys, from a vulnerable server's memory. Whereas a format string vulnerability is a type of programming error that can be exploited to manipulate the formatting of data output, leading to potential information disclosure or code execution. The severity of a bug depends on various factors, including the impact, potential exploits, and the context in which it occurs. While both Heartbleed and a format string vulnerability can be serious, their specific implications may differ.

Question 3

i. Two examples of real attacks that could have been prevented if software updates were taken more seriously are:

1. WannaCry Ransomware: In 2017, the WannaCry ransomware spread rapidly across the globe, infecting hundreds of thousands of computers. The attack exploited a vulnerability in the Windows operating system for which Microsoft had released a security patch two months prior to the attack. Organizations and individuals who had not installed the patch became victims of the ransomware. If software updates were taken more seriously, and the security patch had been applied promptly, the WannaCry attack could have been prevented.
2. Equifax Data Breach: In 2017, Equifax, one of the largest credit reporting agencies, suffered a massive data breach that exposed sensitive personal information of approximately 147 million individuals. The breach was caused by a vulnerability in the Apache Struts web application framework. A patch to fix the vulnerability had been available for two months before the breach occurred, but Equifax failed to apply the update. If the software update had been implemented in a timely manner, the data breach could have been avoided.

ii. Antivirus software is often rated lower in effectiveness by experts compared to non-experts because malware can employ various techniques to evade or bypass antivirus detection. Some ways a malware can defeat antivirus software include:

1. Polymorphic Malware: Malware can use polymorphic techniques to constantly change its appearance, making it difficult for antivirus programs to detect based on signature matching. By altering its code or structure, the malware can evade traditional detection methods.
2. Zero-day Exploits: Antivirus software relies on signature-based detection to identify known malware. However, when a new and previously unknown vulnerability (zero-day) is exploited by malware, antivirus software may not have the necessary signatures to detect it, allowing the malware to go undetected.

3. Encrypted or Obfuscated Payloads: Malware authors can encrypt or obfuscate malicious code, making it harder for antivirus software to detect the actual payload. By employing encryption or obfuscation techniques, malware can evade static analysis and signature-based detection.

Experts understand these limitations of antivirus software and recognize that it should be just one layer of defense among multiple security measures, such as patching software, using strong passwords, and employing behavioral analysis and heuristics-based detection methods.

iii. A password manager offers several benefits for improving login security. From the webmaster's perspective, even if the web server has strong defenses, an attacker can exploit a common weakness: password reuse. If a user does not use a password manager and employs the same password across multiple websites, the attacker can take advantage of compromised credentials from one site to gain access to another.

The attack vector would involve the attacker targeting a website where the user's login name is known. The attacker would attempt to gather leaked password databases from other websites and use those passwords to try and log in to the targeted website. Since many users reuse passwords, there is a high probability that the compromised password from another site would also grant access to the targeted website. By using a password manager, individuals can generate unique, strong passwords for each website, eliminating the risk of password reuse and mitigating the impact of such an attack vector.