CMPT 403

Assignment 1 Written

1) Question 1
    a. Question
        i. CIA Violations
            1. Integrity: The victim’s computing resources are used to mine cryptocurrencies for the attacker.
            2. Availability: The availability of the victim's computing resources is reduced as they are being used for crypto mining.
        ii. Malware Classification
            1. Spread through Network: Background scripts are being that client clients on the network, showing a failure of web application
        iii. Counter-Measure
            1. Practice safe coding during the developmental phase of the web application. Frequent testing increases the chances of finding errors, bugs or vulnerabilities. Clients can use safe web tools to prevent malicious background scripts
    b. Question
        i. CIA Violations
            1. Integrity: RSA Security uses Dual_EC_DRBG causing its cryptographic system to be at risk.
        ii. Malware Classification
            1. This goes with the idea of Planted malware as we can expect that someone at NSA could have planted this. Or it could have a vulnerability that had not been exposed yet.
        iii. Counter-Measure
            1. Make the application open source for testing instead of just NSA being the sole editor. Use alternative algorithms that don’t use Dual_EC_DRBG random generator.
    c. Question

i. CIA Violations

1. Integrity: The cell is now being exposed to attackers causing risk.
2. Confidentiality: Personal info is being leaked to the attacker using surveillance software. The malware intercepts communications and data, violating confidentiality.
3. Availability: Surveillance Software uses the phone resources disrupting regular phone usage.

ii. Malware-Classification

1. Trojan: Sending the attack as a GIF file

iii. Counter-Measure

1. Regular updates to the phone and applications
2. Installing an anti-virus that detects trojan files efficiently (scans for virus “signatures”.

d. Question

i. CIA Violations

1. Integrity: Gaining Control of target devices can allow modification of data.
2. Confidentiality: Control of the devices causes confidential data about the target to be leaked to the attacker.
3. Availability: The device can be used in DDoS attacks, affecting its availability.

ii. Malware-Classification

1. Uses network as the target device acts as a medium for DDoS attack

iii. Counter-Measure

1. Apply security patches provided by the vendor to fix the vulnerability. Implement network security measures such as firewalls and intrusion detection systems to monitor and block suspicious traffic.

2. Question 2

I. Some buffer overflow attacks do not overwrite any return address at all

i. True: As we noticed in the programming exercise of this assignment, not all buffer overflow attacks overwrite return addresses. Some can be used to change certain variables which allows access to the systems.

II. Minimizing privileges in critical programs can help mitigate the impact of buffer overflow attacks.

i. True: Even if a buffer overflow attack succeeds, the impact can be significantly reduced if the exploited program runs with minimal privileges.

III. Return-oriented programming is able to defeat stack canaries.

i. True: ROP does not rely on overwriting the return address directly but instead uses existing code snippets (gadgets) ending in a return instruction to perform malicious operations.

IV. XSS attacks usually require the attacker to gain full control over the web server first.

i. False: XSS exploits vulnerabilities in web applications that allow the attacker to inject malicious scripts into web pages viewed by other users. So, when the target loads the web page, the malicious can then be executed.

V. If there is a format string vulnerability in OpenSSL, it would be a more serious bug than Heartbleed.

i. False: It depends on the exact nature and the context in which OpenSSL could be exploited. So, we can’t say whether format string vulnerability would be more damaging or not.

3. Question 3

I. Examples

1) WannaCry Ransomware Attack: ransomware attack targeting computers running Microsoft Windows by encrypting data and demanding ransom payments in Bitcoin. Windows had patched up the vulnerability with an update but older versions weren’t immune to the attack.

2) Equifax Data Breach: The attackers exploited a vulnerability in Apache Struts, a widely used web application framework. The vulnerability (CVE-2017-5638) had been identified and patched

two months before the breach, but Equifax failed to update their software in time.

II. Description of malware bypassing antivirus

1) Using Polymorphic malware: This type of malware changes its code each time it infects a new system. By altering its signature, it can evade detection by traditional signature-based antivirus programs, which rely on known patterns to identify malicious software.
2) Using Fileless Malware: This malware does not write any files to the disk, making it difficult for antivirus software to detect. It typically operates by injecting malicious code directly into memory or exploiting legitimate tools like PowerShell to execute its payload.
3) Using Rootkits: Rootkits can intercept and modify system calls, masking the presence of malicious files and processes
4) Using Encrypted Malware: We can hide the true nature of malware using encryption

III. Password Manager

1) Password Manager helps a user generate, stores, and fill in strong, unique passwords for each of their accounts. People often don’t use a password manager and end up using simple, reusable passwords on multiple sites causing a risk.

a. Reusing password: We assume that an attacker has a user’s username but not the password. If users reuse passwords, an attacker who obtains credentials from one compromised site can access accounts on other sites where the same password is used. Password manager prevents this by generating unique passwords for a user.

b. Phishing attacks: Phishing attacks involve tricking users into entering their credentials on a fake website that looks like a legitimate one. Users might not notice subtle differences in URLs and enter their passwords on malicious sites, giving attackers access to their accounts. Password managers automatically fill in credentials only on the correct, legitimate websites

c. Simple, common passwords with brute force attack: Using simple and common passwords like “123456789” or “abcdefgh”, puts a user at risk of being compromised. Since the attacker can try these passwords using scripts, they can easily obtain a user’s account.

d. Keyloggers: Having access to a user’s device, an attacker might place a keylogger to obtain passwords for a user’s account.

e. As we learnt in class, using a password that is hard to remember but easy to guess makes it more likely to be exposed. A password manager helps by generating a high-entropy password. A better option is to use random words that form a memory for a user. Random words give us a higher degree of entropy and are easy to remember.