Exercise – 5

Abdurrehman Syed

2308546

Task – 1

Threat Events

1. Intrusive Application Practices:

- Apps may collect excessive personal data, track user behavior, or have security vulnerabilities that can expose sensitive information.
- **Example:** Apps with hidden permissions or deceptive UIs.

2. Account Credential Theft Through Phishing:

- Attackers utilize fake emails or messages that deceive users to give away work account login credentials.
- **Example:** emails impersonating legitimate organizations.

3. Outdated Phones:

- Older devices might have unsupported operating systems and/or security patches, thus becoming highly prone to attacks.
- **Example:** Devices that haven't received recent security updates.

4. Sensitive Data Transmissions:

- Transmission of sensitive data through unencrypted or insecurely connected networks.
- **Example:** Sending sensitive information over public Wi-Fi without encryption.

5. Brute-Force Attacks to Unlock a Phone:

- Attackers guessing a device's passcode / PIN through repeated attempts.
- **Example:** Using automated tools to try different combinations.

6. Application Credential Storage Vulnerability:

- Applications may insecurely store user credentials, which could potentially leak if the device is compromised.
- **Example:** Apps that don't use strong encryption for password storage.

7. Unmanaged Device Protection:

- Devices may not be sufficiently protected with antivirus software, firewalls, and timely updates.

- **Example:** Devices without latest antivirus or firewall protection.

8. Lost or Stolen Data Protection:

- Sensitive data may be exposed if a device is lost or stolen, especially if it doesn't have adequate data protection measures.
- **Example:** Devices without remote wipe or data encryption options.

9. Protecting Enterprise Data from Being Inadvertently Backed Up to a Cloud Service:

- Users may mistakenly back up work data to personal cloud storage accounts and leak sensitive data.
- **Example:** Syncing company files to a personal cloud storage service.

Task – 2

Foreshadow (CVE-2018-3615): A vulnerability leaking information from an L1 cache using speculative execution. It can be exploited in one of the following ways: by forcing a program to speculatively read data from a memory location for which that program does not have permission; if such data happens to be in the L1 cache, leakage through access patterns from the cache might occur. The primary target of this bug is Intel CPUs. The solution involves updating the microcode and randomization of kernel memory allocation.

RIDL (CVE-2018-12130): It makes use of speculative execution to steal information from the register file of a victim process. Like Foreshadow, RIDL tricks a program into speculatively reading a register to which it is not entitled. In case the value is in the register file, the processor may leak information via side-channels. The RIDL line of attack primarily targets AMD CPUs. The mitigations involve updating the microcode and modifying compilers.

ZombieLoad (CVE-2018-12126): This attack uses speculative execution to leak information from the memory of a victim process. ZombieLoad leverages a situation where a processor speculatively loads data from memory, even if the load operation is ultimately aborted. Carefully crafting such a memory access pattern may trick the processor into revealing information about the data it speculatively loaded. ZombieLoad affects many different CPU architectures from Intel, AMD, and ARM. Mitigations include microcode updates and kernel memory allocation randomization.

Task – 3

1. Common OS Vulnerabilities and Mitigations

Malware and Viruses

Harm: Data breaches, corruption of files, system corruption, and security compromise.

Mitigations

Windows: Windows Defender (built-in antivirus), third-party antivirus software, regular updates.
macOS: XProtect (built-in antivirus), third-party antivirus software, regular updates.
Linux: Use of tools like ClamAV or Bitdefender.

2. Exploiting Software Vulnerabilities

Harm: Unauthorized system access, executing malicious code, and stealing sensitive data.

Mitigations

OS-level: OS-level Regular operating system updates, security patches, and vulnerability scanning.
Software-level: Avoid using obsolete or unsupported software.

3. Phishing and Social Engineering

Harm: It can trick users into providing sensitive information, clicking on links to malware hosting sites, and downloading malware.

Mitigations

OS-level: awareness training for users, enforcement of good password policies.
External tools: Phishing simulation tools, security awareness training programs.

4. Drive-by Downloads

Harm: It automatically downloads malicious software onto a user's device without the user knowing or giving permission.

Mitigations

OS-level: Use only a reputable web browser with built-in security, do not click on suspicious links or download files from untrusted sources.
External tools: Ad-blockers, content filters.

5. Zero-Day Exploits

Harm: The vulnerabilities exploited have not been known to the vendor of the software, hence patching is very hard right away.

Mitigations
OS-level: Regular update with security patches and vulnerability scanning.
External tools: IDS - Intrusion Detection Systems, SIEM - Security Information.

6. USB/Removable Media Attacks
Harm: It can introduce malware, viruses, or unauthorized access to the system.

Mitigations
OS-level: Disable autorun for removable media, scan removable media before accessing.
External tools: Removable media control software.

7. Password Cracking
Harm: It can compromise accounts and obtain unauthorized access to sensitive information.

Mitigations
OS-level: Strong password policies, password complexity requirements.
External tools: Password managers, multi-factor authentication (MFA).

Task – 4

Application Logs

- **Information:** Events and actions relevant to a specific application are tracked here, including errors, warnings, and user interactions.
- **Locations:**
  - **Windows:** Default location is the application directory or %APPDATA%.
  - **macOS:** This can usually be found under the application container directory or under ~/Library/Logs.
  - **Linux:** It depends on your distribution, but for the most part, it can be found in /var/log/application-name.
- **Threats:** Application-specific vulnerabilities, unauthorized access, performance issues.

Event Logs

- **Information:** Track events occurring system-wide, including security events like hardware failures and software installation.
- **Locations:**
  - **Windows:** In %SystemRoot%\System32\winevt\Logs.
  - **macOS:** Found in /var/log.

    - **Linux:** These logs are normally kept in /var/log/messages, /var/log/syslog, etc.
- **Threats:** Security breaches, system failures, hardware malfunctions.

Service Logs

- **Information:** Events and activities generated related to services running on the system, which includes network, print, and application services.
- **Locations:**
    - **Windows:** Normally kept in a folder containing the service or %SystemRoot%\\System32\\Logs.
    - **macOS:** Mostly in /var/log/system.log or /var/log/specific-service.log.
    - **Linux:** Normally in /var/log/specific-service.log.
- **Threats:** Service failures, performance issues, unauthorized access.

System Logs

- **Information:** Record system-wide events, such as boot processes, kernel messages, and hardware interactions.
- **Locations:**
    - **Windows:** Located in %SystemRoot%\System32\winevt\Logs.
    - **macOS:** Found in /var/log.
    - **Linux:** Typically stored in /var/log/messages, /var/log/syslog, and other related files.
- **Threats:** System failures, hardware malfunctions, security breaches.

Monitoring Logs on Your Personal Computer

The following are some ways to monitor logs from your personal computer:

- **Built-in tools:** Windows Event Viewer, macOS Console, or Linux's journalctl command.
- **Third-party tools:** Log management software like Splunk or Graylog
- **Scripting:** Use scripts (e.g., PowerShell, Bash)

Microsoft Documentation:
https://learn.microsoft.com/en-us/windows/win32/wes/windows-event-log-reference
Apple Support: https://support.apple.com/guide/console/welcome/mac
Linux Documentation:
https://wiki.archlinux.org/title/Systemd/Journal
Splunk: https://www.splunk.com/
Graylog: https://graylog.org/