FIT2093 Tutorial 10

Topics

- Attacks on single devices
- Web-application hacking
- Network-based attacks

Review Questions

1. What is a *buffer overflow* and why can it be potentially used to attack a system? Explain in terms of abstract concepts (Input, Storage, Memory content, Memory addresses, etc.). What needs to be done at development time to prevent buffer overflow attacks? What can be done at run-time (or compile time).

2. A current worm has distributed ransomware via a weakness in the SMB protocol on Windows computers. Explain why a properly configured firewall on a computer could have prevented the infection of this particular computer. SMB is a protocol for providing access to shared filesystems or other resources. Explain why a firewall-based protection might not have been possible for a server in an enterprise network.

3. Cookies can be used to identify a particular session between client and server. In combination with a TLS tunnel, cookies can provide a good solution for session identification, if the browser does not provide the cookie to another server, which it usually should not do. Why could an XSS attack still enable an attacker to take over the session. Read https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) to learn about other possible XSS Attack Consequences and go through the examples.