University of Oslo
INF3510 Information Security
Spring 2017
Workshop Questions

Lecture 12: Application and Development Security

Question 1

a. What is the Cyber Kill Chain?
b. What are the steps of the cyber kill chain?

Answer

a. The Cyber Kill Chain consists of the steps that are typically part of an APT (Advanced Persistent Threat). The term 'Kill' refers to the fact that this type of attack can be 'killed' (stopped) at any step in the chain. The earlier the attack can be stopped, the better.
b. The steps of the Cyber Kill Chain are:
   - **Reconnaissance:** The threat agent collects information about the potential victim, with the aim of finding vulnerabilities and opportunities for attack.
   - **Weaponisation:** The threat agent constructs malware based on e.g. exploits, packaged in some form suitable format that can be delivered to the victim. The format can e.g. be a pdf document or a media file.
   - **Delivery:** The malware can e.g. be carried as attachments to deceptive email messages that are try to trick the recipient into opening or installing the malware.
   - **Exploitation:** Assuming that the victim recipient has been deceived/penetrated and the malware has been opened/installed, the malicious functionality takes effect.
   - **Installation:** The malicious effect of exploits is typically to download a backdoor from a remote server. After this step the attackers have remote access to the compromised system.
   - **Command & Control:** The attackers explore the network of the infected system, move laterally inside the network to other systems, take steps to hide, and identify resources to steal or disrupt.
   - **Action/Exfiltration:** Data is collected, prepared and is sent out of the network, to servers controlled by the attackers. If sabotage is the attacker's goal, disruptive actions are taken.

Question 2

a. In general terms, how does a worm propagate?

Answer

c. Worms propagate by **1)** Searching for other systems to infect by examining host tables or similar repositories of remote system addresses. **2)** Establishing a connection with a remote system. **3)** Copying itself to the remote system and cause the copy to be run.

Question 3

a. What is a botnet?
b. What is a DDoS, and how can a botnet be used to mount a DDoS attack?
c. Describer two other attacks that can be executed with botnet.

Answer

a. The term “botnet” is generally used to refer to a collection of compromised computers (called bots or zombie computers) running software, usually installed via drive-by downloads exploiting web browser vulnerabilities, worms, Trojan horses, or backdoors, under a common command-and-control infrastructure.
b. A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service. When this attack comes from a single host or network node, then it is simply referred to as a DoS attack. A more serious threat is posed by a DDoS attack. In a DDoS attack, an attacker is able to recruit a number of hosts throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the target. A botnet is precisely a set of hosts that can be coordinated for DDoS attacks.
c. Botnets are also used for spamming and for collecting identity credentials.

Question 4

a. What is a buffer overflow attack, and how can it be prevented?
b. What is an SQL injection attack and how can it be prevented?
c. What is a Cross-Site Scripting attack, and how can it be prevented?

Answer

a. In computer security and programming, a buffer overflow, or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory reserved for it. The extra data overwrites adjacent memory, which may contain other data, including program variables and program flow control data. This may result in erratic program behaviour, including memory access errors, incorrect results, program termination (a crash), or a breach of system security.
b. SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks can be prevented by not allowing user input to be directly embedded in SQL statements. Instead, parameterized statements must be used (preferred), or user input must be carefully escaped or filtered.
c. Cross-Site Scripting: (Acronym XSS) An attack technique that forces a web site to echo client-supplied data, which execute in a users web browser. When a user is Cross-Site Scripted, the attacker will have access to all web browser content (cookies, history, application version, etc). XSS attacks do not typically directly target the web server or application, but are rather aimed at the client. The web server is merely used as a conduit for the XSS data to be presented to the end client. XSS can be prevented by always sanitizing input to web servers.

Question 5

a. What is the meaning of the abbreviation OWASP ?
b. What is the main goal of OWASP ?
c. What is the OWASP Top 10 ?
d. What is nr.1 in the OWASP Top 10 ?
e. What is the reason why nr.1 has been at the top for many years ?
f. What is the meaning and purpose of OWASP ASVS ?

Answer

a. OWASP: Open Web Application Security Project
b. OWASP promotes security awareness and security solutions for Web application development.
c. The OWASP Top 10 describes the most prevalent security vulnerabilities in current web application.
d. SQL injection is the nr.1 application security vulnerability found on the Internet.
e. SQL injection should not be the nr.1 security vulnerability, because there are simple solutions to prevent SQL injection. The reason why it is still nr.1 is for example that application developers are ignorant or lazy or both.
f. OWASP ASVS (Application Security Verification Standard) specifies requirements for application-level security, and provides and maintains many free tools for scanning and security vulnerability fixing

Question 6

a. Mention the 6 basic stages of the SDLC (Software Development Life Cycle)
b. Mention the 3 main elements of SDL (Secure Development Lifecycle)
c. SDL requires security related tasks to be included in each stage of the SDLC. In which SDLC-stage is fuzzing done ?

Answer

a. SDLC stages: 1) Requirements Specs, 2) Design, 3) Implementation, 4) Testing, 5) Deployment, 6) Maintenance

b. SDL elements:

    1. Include security related tasks in each stage of the SDLC
    2. Security education for system engineers
    3. Metrics and accountability to assess security of system

c. Fuzzing is done in the testing stage.

Question 7

a. *Waterfall* and *agile* are two different SDLC (Software Development Life Cycle) models. To which of these can Microsofts SDL (Secure Development Lifecycle) best be applied ?
b. What is Phase-1 in Microsoft SDL, and why is it needed for building secure software ?
c. How can universities contribute to secure software and to a secure IT infrastructure ?

Answer

a. Microsoft SDL fits best with the waterfall SDLC model.
b. Phase-1 of SDL is security training, which is essential to make a team able to develop secure software.
c. Software engineers should learn how to make secure software during their studies when they learn software development. IT education programs without mandatory security training necessarily produces IT experts and software engineers who are security analphabets and who therefore will develop vulnerable systems that in turn will contribute to an insecure IT infrastructure. Universities that offer IT programs without mandatory security training are part of the problem of weak cybersecurity. Universities must become part of the solution.

Question 8

a. What is the meaning of the abbreviation OpenSAMM ?
b. What is the purpose of OpenSAMM ?
c. What is the structure of OpenSAMM ?

Answer

a. OpenSAMM: Open Software Assurance Maturity Mode
b. OpenSAMM offers a framework for helping software development organisations to become better at making secure software, and a method for an organisation to assess how good (how mature) it is secure software development.
c. OpenSAMM specifies 4 top level categories called *Business Functions*. Each top level category consists of 3 practices, so that there are a total of 12 practices.