



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

Answer

- a. 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.
- b. Cross-Site Scripting: (Acronym XSS) An attack technique that forces a web site to echo client-supplied data, which execute in a user's 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. In what way is agile different from waterfall in system development.
- b. How can security be integrated in agile system development.

Answer

- In waterfall system development, all the functionality to be developed must be specified before the programming starts. In contrast, agile system development is centered around a series of sprints that typically last a few weeks. During each sprint the software development team implements a small set of functions or “user stories”. New functions and user stories can be specified along the way.
- In secure agile there must be security oriented tasks
 - at the initiation of the project (identify stakeholder security priorities and concerns, define security requirements),
 - during each sprint (identify threat scenarios, and remove vulnerabilities to stop threat scenarios),
 - at the final testing of the system (test/evaluate that security requirements are met).

