Topic 5 Discussion 1

Define and contrast attack surfaces, attack vectors, and attack trees. Provide an example of each.

Hello Class,

Attack Surface

The attack surface refers to the total sum of all the points (or surfaces) in a system or network where an unauthorized user (an attacker) can attempt to enter or extract data. It includes all vulnerabilities that can be exploited.

Contrast: The attack surface represents the scope of potential vulnerabilities in a system.

Example:

In a web application, the attack surface includes:

User input fields (e.g., login forms, search boxes)

APIs that interact with the application

Third-party integrations (e.g., payment gateways)

Attack Vector

An attack vector is a path or means by which a hacker can gain access to a computer or network to deliver a payload or malicious outcome. It is the method used to exploit vulnerabilities within the attack surface.

Contrast: While the attack surface represents all potential entry points, attack vectors are specific methods or paths that exploit those vulnerabilities.

Example:

A common attack vector is phishing:

An attacker sends an email that appears to be from a legitimate source, tricking the user into clicking a link that leads to a malicious website.

Attack Tree

An attack tree is a graphical representation of the various ways an attack can be carried out against a system. It breaks down potential attack paths into sub-branches, illustrating the methods, resources, and steps required to achieve a specific attack goal.

Contrast: Attack trees provide a structured way to analyze the different methods of attack, whereas attack surfaces and vectors focus more on the vulnerabilities and the paths taken to exploit them.

Example:

An attack tree for gaining unauthorized access to a network might include:

Root Node: Gain unauthorized access

Branch 1: Exploit vulnerabilities

Sub-branch 1.1: SQL injection

Sub-branch 1.2: Cross-site scripting (XSS)

Branch 2: Use social engineering

Sub-branch 2.1: Phishing

Sub-branch 2.2: Pretexting

References:

Attack Vector vs Attack Surface. (2020, May 28). Balbix. https://www.balbix.com/insights/attack-vector-vs-attack-surface/

Attack Vector vs Attack Surface: The Subtle Difference. (2023, February). Trend Micro. https://www.trendmicro.com/en\_us/research/23/a/attack-vector-vs-attack-surface.html

IBM. (n.d.). What is Attack Surface? | IBM. Www.ibm.com. https://www.ibm.com/topics/attack-surface

What are attack vectors, attack paths and attack surfaces? (2023, July 7). https://appcheck-ng.com/what-are-attack-vectors-attack-paths-and-attack-surfaces/