Exercise 3 - Additional Cybersecurity Attack Types

We have already run through practical demonstrations of a Cross-site scripting attack and an SQL Injection Exploit. These are just two attack types that may be used by a malicious third party however, and a Cyber Security Analyst needs to be aware of many different avenues an attacker may use to penetrate a network.

In this exercise, additional Cybersecurity attack types will be discussed.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Additional Cybersecurity Attack Types

Your Devices

This exercise contains supporting materials for CySA+.

Extensible Markup Language (XML) Attack

An Extensible markup language (XML) attack occurs when an application that parses XML input is incorrectly configured and can lead to the disclosure of confidential information, Denial of Service for the application or Server Side Request forgery.

This type of attack can be prevented by ensuring the best coding practices are met and that the web application has been correctly configured.

Overflow Attack

There are several types of Overflow attacks that can occur. These include the following:

- **Buffer Overflow attack:** These types of attacks the attacker causes the application to use more memory than normal, which will result it flowing into adjacent memory space. Causing the corruption or overwriting the data in the particular memory space. When a Buffer overflow attack occurs, it may cause the application to crash or give a malicious user access to perform malevolent actions.
- **Integer Overflow Attack**: Very similar to a buffer overflow attack, an Integer overflow attack occurs when an arithmetic calculation occurs in the application, and the result is too large to be stored in the allocated storage resulting in an Integer overflow. Allowing an attacker to gain access to the application.
- **Heap Overflow Attack**: Heap is storage that is allocated at runtime or when an application starts up. If this storage is compromised, it can cause that the application will crash due to insufficient storage space.

Remote Code Execution

A remote code execution attack occurs when an attacker executes code remotely on a vulnerable system. By executing the code, an attacker will then gain access and control of the remote system from anywhere in the world. This type of code can be executed when the user unknowingly installs malware on the computer system being misled through a malicious email.

Directory Traversal

This is a HTTP attack where the attacker gains access to restricted directories on a web server. This type of attack occurs when proper security measures on the webserver are not implemented. For example, securing the resources using Access Control Lists (ACL) to prevent unauthorized access.

Privilege Escalation

Privilege escalation is conducted by exploiting flaws in the design of a specific operating system or software application. The flaw is used to gain elevated access to resources in the operating system, which is normally restricted to non-privileged users. When access is gained to these restricted resources, the malicious users will then be able to make changes that were not possible before.

Another type of privilege escalation is when a privileged user account is compromised and then used to escalate the privileges of other user accounts to perform malicious activities.

Password Spraying

A password spraying attack is conducted by gathering a list of usernames from an organization and then using a single password to try to access these specific user accounts.

The user account names can be harvested by using social engineering or phishing scams. The attack is based on the assumption that users use weak passwords, which can be easily guessed by the attacker.

Credential Stuffing

Credential stuffing relates to gaining access to a user account and then using the same credentials to gain access to other systems on the network. These types of attacks are commonly used to gain unauthorized access to online platforms. An example is breaching a user’s Facebook account and then using the same credentials to try and access the user’s email address or internet banking site.

Impersonation

Impersonation in Cybersecurity, the attacker, will impersonate a trusted individual from the company to trick the user in divulging sensitive information, for example, usernames or passwords. An impersonation attack can be conducted via email, telephone, or even instant messaging.

Man-in-the-Middle-Attack

Man-in-the-middle attacks are conducted when the attacker gains unauthorized access to the network and then intercepts network traffic between computers and servers without the user’s knowledge. The captured network traffic can then be analyzed by the attacker to identify sensitive information, for example, passwords or usernames.

Session Hijacking

Session hijacking occurs when a user connects to, for example, a server remotely, and the attacker takes control of the specific session from the user. It is very similar to a Man-in-the-middle attack. With session hijacking, the attacker captures the user session ID and uses it as an authentication mechanism for the remote server. As long as the user is logged into the server, the Session ID will be valid, and the attacker will have access to the resources of the user.

Rootkit

Rootkit exploits rely on malicious software being installed on a user’s computer. The malicious software or malware enables the attacker to gain access to the system to gather sensitive information of the user, for example, a user’s credit card details or passwords to banking sites.