

Professional Skills
Agile Fundamentals
Jira
Git
Databases Introduction
Java Beginner
Maven
Testing (Foundation)
Java Intermediate
HTML
CSS
Javascript
Spring Boot
Selenium
Sonarqube
Advanced Testing (Theory)
Cucumber
MongoDB
Express
NodeJS
React
Express-Testing
Networking
Security
<div><div></div>Security Basics</div>
<div><div></div>Authentication and Authorization</div>
<div><div></div>Security Attacks</div>
<div><div></div>Passwords</div>
<div><div></div>Hashing vs Encrypting vs Encoding</div>
<div><div></div>Introduction to DevSecOps</div>
<div><div></div>Pen Testing, DAST & SAST</div>

Security Attacks

Contents

- [Overview](#)
- [Attacks](#)
 - [DDOS](#)
 - [MitM](#)
 - [Phishing](#)
 - [Drive By](#)
 - [Password Attacks](#)
 - [Malware](#)
 - [Social Engineering](#)
 - [SQL Injection](#)
 - [Cross-site Scripting_\(XSS\)](#)
- [Tutorial](#)
- [Exercises](#)

Overview

In this module we will briefly look at different security attacks.

Attacks

DDOS

A Distrubuted Denial Of Service attack is where a person or group of people make a large number of requests to a website, hoping that the volume will overload the servers and cause the website to go down.

One person can use zombie machines to make a large number of attacks or groups of people can coordinate to make many requests together.

MitM

A Man In The Middle attack is where an attack infiltrates a connection between 2 hosts and reads the data being transmitted between them.

This connection can be between a client and a server so if a user enters some sensitive information into a website e.g. Password.

Someone performing a man in the middle attack would be able to read that data.

We can encrypt our data to minimise the risk from these types of attacks.

Phishing


A phishing attack is where an attacker tries to get someone to click a harmful link or reveal sensitive data by appearing as a legitimate source e.g. HMRC or British Gas.

The link will then redirect the user to some sort of Malware even though it looks like a normal, innocent link.

Drive By

A Drive By attack is where an attacker injects a site with some malicious code trying to spread malware to end users.

If a website is not secure an attacker could add some code that adds a button to the page and if an end user clicked that button it could do many different things but normally it would download some malware or a virus.

 Introduction to OWASP
Cloud Fundamentals
AWS Foundations
AWS Intermediate
Linux
DevOps
Jenkins Introduction
Jenkins Pipeline
Markdown
IDE Cheatsheet

Password Attacks

A password attack is where an attacker attempts to get a users password or sensitive data through a number of methods.

Brute Force Attack

This is a kind of password attack where the attacker attempts every combination of characters in the hope of coming across the correct password.

e.g. Attempt 1: AAA, Attempt 2: AAB etc

Dictionary Attack

A dictionary attack is similar to a Brute force attack but instead of trying every possible combination, it will try common phrases first, e.g. Password, root etc.

Malware

Malware attacks is where **MAL**icious Soft**WARE** is installed onto a victims computer.
As shown with the previous attacks, the methods in which they get it installed can vary.
Malware can come in many different forms e.g. viruses, ransomware.
This software will in some way stop the user being able to use or access their computer.

Social Engineering

Social Engineering targets the user behind the computer rather than the computers themselves.
This is where an attacker will try to manipulate a person into giving up information or giving the attacker access to some information.
This kind of attack relies on a few things, like human error, carelessness or luck.

SQL Injection

SQL injection is an attack used against data driven applications. The attack exploits SQL statements that web applications use to communicate to the database. It allows attackers to use SQL queries to expose hidden data, this can include passwords, credit card details, or personal information.

Cross-site Scripting (XSS)

Cross-site scripting or XSS is an attack that exploits interactions that the user makes with an application. The attacker is able to make use of vulnerabilities in the web application, usually comment fields or forms, in order to inject scripts into the server. This attack is often used on blogs or social networks so that the injected malware is shared.

Tutorial

There is no tutorial for this module.

Exercises

Take a look at this [article](#) about a DDOS on the website Github.