Module 4: CS - Securing Web Applications Services & Servers

1. Explain MAC spoofing and Email spoofing

Ans: MAC Spoofing : MAC Spoofing is a type of attack used to exploit flaws in the authentication mechanism implemented by wired and wireless networking hardware.

Email spoofing : [Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they know or trust.](https://www.bing.com/ck/a?!&&p=e703cd95225742237fb97b3b5eb8e343a4614ed0312f522a2216f250754da138JmltdHM9MTczMjQ5MjgwMA&ptn=3&ver=2&hsh=4&fclid=1dcdf568-3d87-6e75-32ad-e1b43c1c6f7f&psq=Explain+Email+spoofing+&u=a1aHR0cHM6Ly93d3cucHJvb2Zwb2ludC5jb20vdXMvdGhyZWF0LXJlZmVyZW5jZS9lbWFpbC1zcG9vZmluZw&ntb=1)

1. Perform practical of MITM tool and social engineering Tool

Ans: Done in Lab.

1. Explain Kali linux tool SYN Flooding Attack using Metasploit

Ans: TCP SYN flood is a type of Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

1. Find online email encryption service

Ans: Done in Lab.

1. Types of Firewall

Ans: Types of firewall:

* Packet Filters
* Stateful Inspection Firewalls
* Application Layer Firewalls
* Circuit-level Gateways
* Software Firewall
* Hardware Firewall
* Cloud Firewall

1. Explain Evading Firewalls

Ans: Done.

● Web Based Hacking

1. What is Session Hijacking Explain with Techniques?

Ans: This is techniques :

* Using Packet Sniffers
* Cross Site Scripting
* IP Spoofing
* Blind Attack

1. Find DoS/DDoS Attack Tools

Ans: [Commonly used DoS/DDoS attack tools include](https://www.bing.com/ck/a?!&&p=fcf105d4371c340076da478a1e3489f5e326ccddbc4394f5450fb7791cd7b7c7JmltdHM9MTczMjQ5MjgwMA&ptn=3&ver=2&hsh=4&fclid=1dcdf568-3d87-6e75-32ad-e1b43c1c6f7f&psq=dos+ddos+attack+tools&u=a1aHR0cHM6Ly93d3cuY2xvdWRmbGFyZS5jb20vbGVhcm5pbmcvZGRvcy9kZG9zLWF0dGFjay10b29scy9ob3ctdG8tZGRvcy8&ntb=1) :

* Low Orbit Ion Cannon (LOIC)
* High Orbit Ion Cannon (HOIC)
* Slowloris
* R.U.D.Y (R-U-Dead-Yet)
* Tools for IP address spoofing
* Ping of Death
* ICMP
* UDP flood and DNS flood attack

1. Explain SYN Flooding Attack with example

Ans: Done in Lab.

1. List of Web App Hacking Methodology

Ans: Introduction to Hacking Web Applications:

* Authentication and Authorization
* XSS – Cross site scripting
* Bypassing blacklists and whitelists
* CSRF – Cross site request forgery
* Unvalidated redirects

1. SQL Injection Methodology

Ans: Done in Lab.

1. Explain sql injection with any tool

Ans: SQL Injection is a security flaw in web applications where attackers insert harmful SQL code through user inputs. This can allow them to access sensitive data, change database contents or even take control of the system. It’s important to know about SQL Injection to keep web applications secure.

1. Explain deference between VA And PT

Ans: Done.

1. How to write vulnerability assessment Report

Ans: Done in Lab.

1. Explain the Zero Day Attacks .

Ans: [A zero-day attack is a malicious act where cybercriminals exploit a previously unknown vulnerability](https://www.bing.com/ck/a?!&&p=a960054589afbc48d7bbdd1ddb3ebaf7badf8105368c51714f51eeea7c46f3f2JmltdHM9MTczMjQ5MjgwMA&ptn=3&ver=2&hsh=4&fclid=1dcdf568-3d87-6e75-32ad-e1b43c1c6f7f&psq=explain+zero+day+attack&u=a1aHR0cHM6Ly93d3cuY2xvdWRkZWZlbnNlLmFpL3doYXQtaXMtemVyby1kYXktYXR0YWNrLw&ntb=1).