CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

INSTITUTE : UIE

DEPARTMENT : CSE

Bachelor of Engineering (Computer Science & Engineering)

WEB AND MOBILE SECURITY (Professional Elective-I)

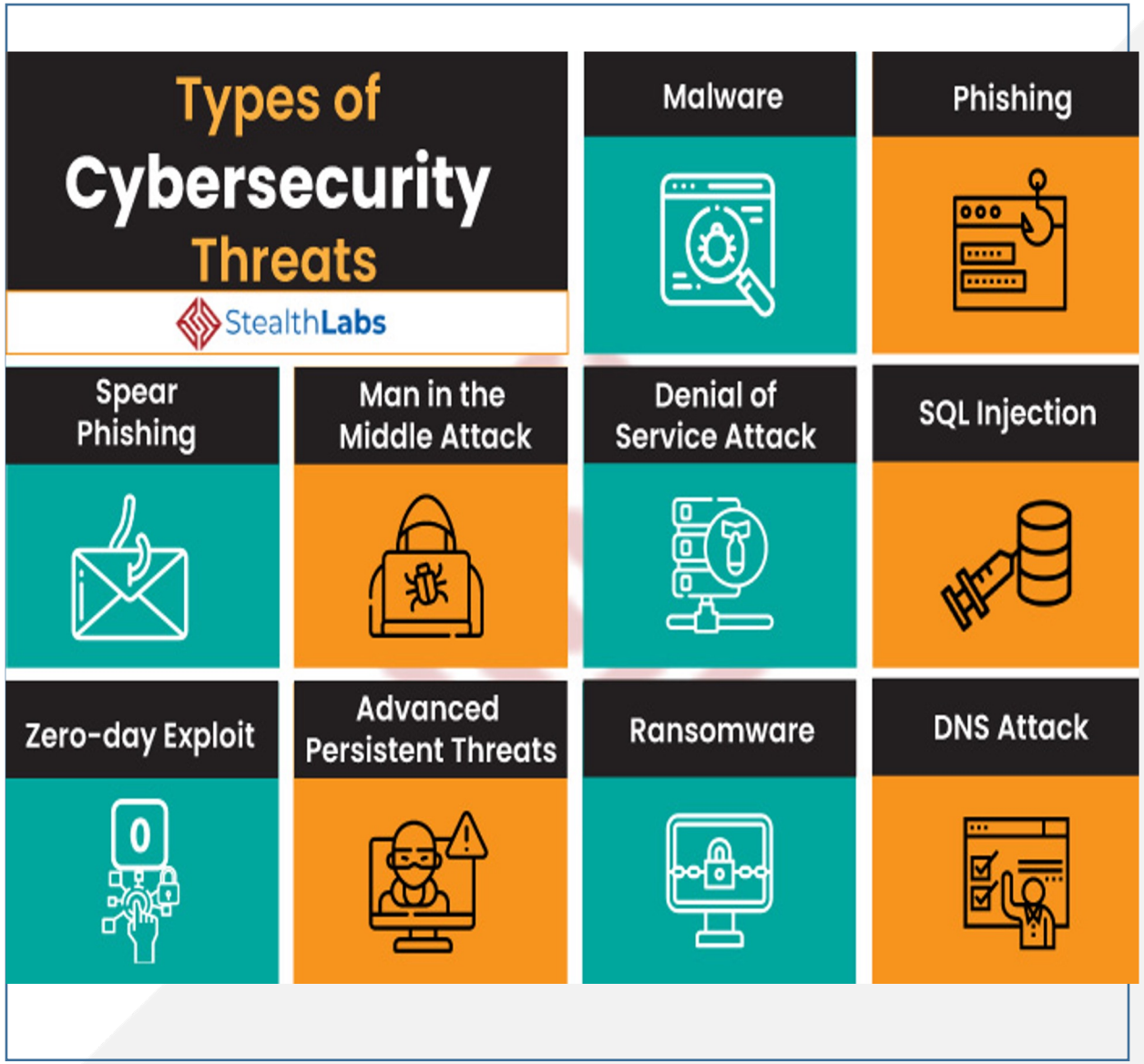
(20CST/IT-333)

TOPIC OF PRESENTATION:

Attacks, detection evasion techniques, and countermeasures for the most popular web platforms, including IIS, Apache, PHP, and ASP.NET.

Lecture Objectives

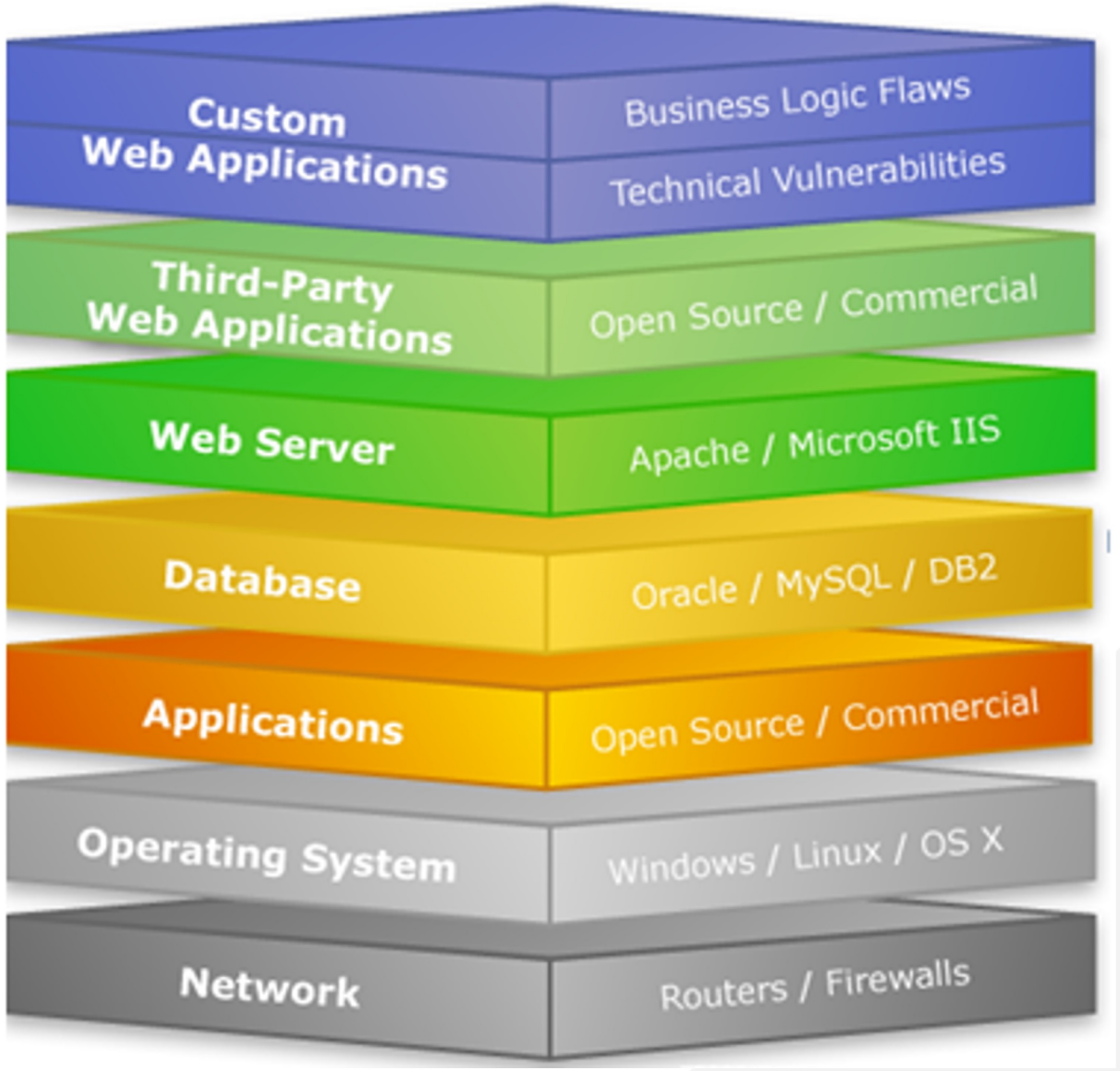
In this lecture, we will discuss:
Web platforms-Attacks,
Detection Evasion Techniques



Web Server and its Types of Attacks

- Websites are hosted on web servers. Web servers are themselves computers running an operating system; connected to the back-end database, running various applications. Any vulnerability in the applications, Database, Operating system or in the network will lead to an attack on the web server. Vulnerability stack of a web server is given below (source: White hat security)
- Denial-of-Service (DoS) / Distributed Denial-of-service (DDoS)
- Web Defacement Attack
- SSH Brute Force Attack
- Cross-site scripting (XSS)
- Directory Traversal
- DNS Server Hijacking
- MITM Attack
- HTTP Response Splitting Attack

https://www.geeksforgeeks.org/web-server-and-its-types-of-attacks/

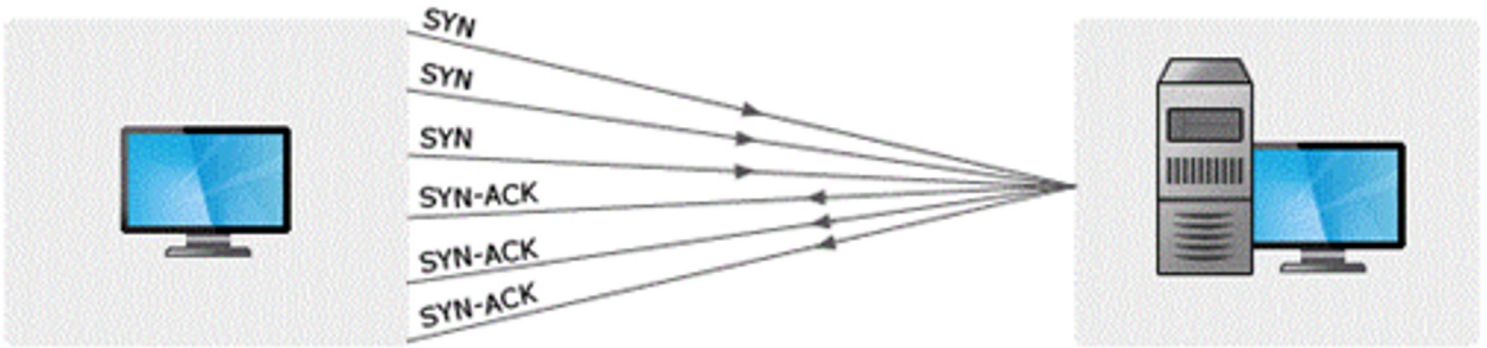

Custom
Web Applications
Business Logic Flaws
Technical Vulnerabilities
Third-Party
Web Applications
Open Source / Commercial
Web Server
Apache / Microsoft IIS
Database
Oracle / MySQL / DB2
Applications
Open Source / Commercial
Operating System
Windows / Linux / OS X
Network
Routers / Firewalls

IIS and Apache : attack types

1. DOS attack:

- An attacker may cause a denial of service attack by sending numerous service request packets overwhelming the servicing capability of the web server, or he may try to exploit a programming error in the application causing a DOS attack.

e.g. buffer overflow attack, SYN flooding, HTTP get Request Flooding, Ping of death.



Non-Infected PC

Web Server not available for legitimate connection

2. Website Defacement:

- SQL injection attacks are used to deface the website. When an attacker finds out that input fields are not sanitized properly, he can add SQL strings to maliciously craft a query which is executed by the web browser. He may store malicious/unrelated data in the database; when the website is requested, it will show irrelevant data on the website, thus displaying a defaced website.

3. Directory Traversal:

- This is vulnerability where an attacker is able to access beyond the web root directory from the application. If he is able to access beyond web root directory, he might execute OS commands and get sensitive information or access restricted directories.

4. Misconfiguration attacks:

- If unnecessary services are enabled or default configuration files are used, verbose/error information is not masked; an attacker can compromise the web server through various attacks like password cracking, Error-based SQL injection, Command Injection, etc.

5. Phishing Attack:

- An attacker may redirect the victim to malicious websites by sending him/her a malicious link by email which looks authentic, but redirects him/her to malicious web page thereby stealing their data.
- There are a lot of other web application attacks which can lead to a web server attack- Parameter form tampering, Cookie tampering, unvalidated inputs, SQL injection, Buffer overflow attacks.

Methodology

Information Gathering:

- Information related to the target server is collected from various sources like
- From websites
- WHOIS information
- Netcraft information
- Banner grabbing
- Port scanning with Nmap.
- Mirroring a website using Htttrack.

Vulnerability Scanning:

- There are automated tools for scanning a web server and applications running on it. The results may show various threats and vulnerabilities on the target web server; these vulnerabilities may later be exploited using tools or manually.
- E.g. Acunetix, Nikto, Vega etc

Password Attacks:

- Guessing/Default passwords
- Brute Forcing
- Dictionary Attacks

Countermeasures

- Update and patch web servers regularly.
- Do not use the default configuration.
- Store configuration files securely.
- Scan the applications running on the web server for all vulnerabilities.
- Use IDS and firewall with updated signatures.
- Block all unnecessary protocols and services.
- Use secure protocols.
- Disable default accounts, follow strict access control policy.
- Install Anti-virus, and update it regularly.
- All OS and software used should be latest and updated.

References:

Books:

1. Hacking Exposed Mobile: Security Secrets & Solutions 1st Edition, Kindle Edition, by Neil Bergman, Mike Stanfield, Jason Rouse, and Joel Scambray
2. Hacking Exposed Web Applications, 3rd edition, Joel Scambray, Vincent Liu, Caleb Sima, Released October 2010, Publisher(s): McGraw-Hill

Video Lectures :

1https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks

2. https://intellipaat.com/blog/what-are-cyber-security-threats/

Reference Links:

1. https://developer.mozilla.org/en-US/docs/Web/Security/Types_of_attacks

2. https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/

https://www.greycampus.com/opencampus/ethical-hacking/web-server-and-its-types-of-attacks

THANK YOU