Faculty of Computer Studies (FoCS)
Sub Committee for Curriculum Development

Format to submit syllabus

Course Name: Advanced Vulnerability Assessment and Penetration Testing

(UG/PG): PG

Number of Credits: 2

Level: 4

Learning Objective(s): The goal of the VAPT course is to demonstrate how to adopt preventive measures against malicious attacks.
The VAPT course prepares individuals in the network security discipline for several certifications from a vendor-neutral perspective.

Pedagogy:

Lectures
Discussion
Case studies
Hands-on lab work

Pre-learning: **S**ound knowledge of Network Infrastructure, Internetworking and Application services

Course Outline:

Sr. No.	Topics	Hours
1	Introduction What is vulnerability research? What is exploit development? Career path in security	1
2	Security Testing Process Methodology Written Contract Open source tools False positives Reporting	2
3	Information Gathering Passive Information Gathering	4

	Search engines, DNS/whois/domains, Google hacking, Social media, Archives, Individual/organization search Active Information Gathering Scanning Types of scanning methods underlying technology behind scanning Fingerprinting operating systems and applications Fingerprinting techniques System Enumeration open source scanners	
4	Web hacking Web application vulnerabilities OWASP and WASC SQL Injection Cross site scripting attacks Cross site request forgery attacks File Upload File inclusion Security misconfiguration Directory traversal Improper error handling	12
5	Buffer overflows What is buffer overflow Types of buffer overflows Reasons for buffer overflows Understanding the process layout Shellcode basics	4
6	Exploitation Introduction Nessus Metasploit	4
7	Firewall IDS/IPS Filter Proxies	3
	Total	**30**

Books Recommended:

Advance Penetration Testing for Highly-Secured Environments By Lee Alan

Parallel/Similar courses the existing curriculum:

S.No.	Name of the course	Institute where it was offered

Name of Member	Prof. Harshad Gune				
Designation	Dy.Director				
Org. / Inst.	SICSR				
Signature					

Name of the Expert:

Signature:

Date: