Faculty of Computer Studies (FoCS)

Course Name: Virtualization and Security

(UG/PG): PG

Number of Credits: 3

Level: 4

Learning Objectives: The major focus of this course is to identify the security gaps in designing the virtual network, resource allocation and suggest probable respective solutions.

Pre-learning:

Pedagogy:

Lectures
Class work discussion

Course Outline:

Sr. No.	Topic	Hours
1	Introduction to Virtualization: Basics of Virtualization Para virtualization Vs Hardware Virtualization, Need for Security in Virtualization, Virtualization System-Specific Attacks: Guest hopping, attacks on the VM (delete the VM, attack on the control of the VM, code or file injection into the virtualized file structure), VM migration attack, hyper jacking.	5
2	Security Concepts: Confidentiality, privacy, integrity, authentication, non-repudiation, availability, access control, defense in depth, least privilege, how these concepts apply in the cloud, what these concepts mean and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud, Securing Hypervisor	4
3	Virtualization System Vulnerabilities: Management console vulnerabilities, management server vulnerabilities, administrative VM vulnerabilities, guest VM vulnerabilities, hypervisor vulnerabilities, hypervisor escape vulnerabilities, configuration issues, malware (botnets etc) Designing Virtual Networks for Security	7
4	Resource Allocation & Sharing techniques in Virtualization, Secure Virtual Machine Isolation in Virtualization	7
6	Technologies For Virtualization: Based Security Enhancement IBM security virtual server protection, virtualization-based sandboxing; Storage Security: HIDPS, log management, Data Loss	9

	Prevention Location of the Perimeter	
7	Security Aspects related with Virtualization: Architectural Considerations, General Issues, Trusted, Cloud Computing, Secure Execution environments and Communications, Micro architectures, Identity Management and Access Control, Autonomic Security.	8
8	Secure Practices in designing Virtual Infrastructure : Legal and Compliance Issues: Responsibility, ownership of data, right to penetration test. Local laws, examination of modern Security Standards (eg PCIDSS), Standards to deal with cloud services and virtualization, compliance for the cloud provider vs. compliance for the customer.	5
	Total	**45**

Books Recommended:

1. Virtualization Security: Protecting Virtualized Environments By Dave Shackleford
2. Virtualization for Security: John Hoopes
3. Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'ReillyMedia Inc, 2009
4. Ronald L. Krutz, Russell Dean Vines, "Cloud Security A comprehensive Guide to secure Cloud Computing" Wiley
5. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing" 2009
6. Vmware "VMware Security Hardening Guide" White Paper, June 2011
7. Cloud Security Alliance 2010, "Top Threats to Cloud Computing" Microsoft 2013
8. Timothy Grance; Wayne Jansen;NIST "Guidelines on Security and Privacy in Public Cloud Computing" , 2011
9. Evelyn Brown NIST "Guide to Security for Full Virtualization Technologies", 2011
10. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/techpaper/vmw-white-paper-secrty-vsphr-hyprvsr-uslet-101.pdf
11. https://cloudsecurityalliance.org/wp-content/uploads/2011/11/virtualization-security.pdf

Suggested Evaluation Methods:

On line Test
Viva
Assignments

Parallel/Similar courses the existing curriculum:

S.No.	Name of the course	Institute where it was offered
1	Cloud Security	Gujarat Technological University
2	Virtualization Security	American Public University
3	Virtualization Security	Berkley University
4	Cloud Security	SICSR

Name of Member	Dr. Tejaswini Apte	Dr. Parag R. Kaveri	Prof. Vivek Deshpande		

Designation	Assistant Professor	Assistant Professor	Visiting Professor		
Org. / Inst.	SICSR	SICSR	SICSR		
Signature					

Name of the Expert:

Signature:

Date: