WEF Academic Year	: 2021-22
Semester	: 1
Category of the Course	: Program Elective Course-II
Course Name & Code	: Operating System and Host Security (4715906)

Prerequisite:

- Operating System Fundamentals.

Rationale:

- This course aims to study, learn, and understand the main concepts of secure operating systems design and Hardware as well as software features that support these systems.
- To understand BIOS boot environments and how they interact with the platform architecture.

Course Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

Course Content:

Sr No	Course Content	No of Hours	%
1	UNIT-I: Introduction Operating System Fundamentals, Concept of Trusted Operating Systems and Secure Operating Systems, Understanding of Trust and Threat Models	06	15
2	UNIT-II: Access Control Fundamentals Protection System – Lampson's Access Matrix, Mandatory protection systems, Reference monitor.	06	15
3	UNIT-III: Multics Multics systems, Multics security, Multics vulnerability analysis	06	15
4	UNIT-IV: Security Analysis in ordinary Operating System Case Study – UNIX and Window Operating System	06	15
5	UNIT-V: Verifiable security goals Information flow concept, Denning's Lattice model, Bell-Lapadula model, BIBA Integrity model, Covert Channels, security kernels – Secure communication process (SCOMP) and GEMINI operating system	06	15
6	UNIT-VI: Secure capability System Fundamentals, Security challenges, Secure Virtual Machine Systems	05	13
7	UNIT-VII: BIOS Introduction, BIOS Identification and trusted platform, Roots of trust, Challenges in bootstrapping trust in secure hardware.	05	12

Reference Book:

1. Trent Jaeger, Operating System Security, Morgan & Claypool Publishers, 2008.
2. Bryan Parno, Jonathan M. McCune, Adrian Perrig, Bootstrapping Trust in Modern Computers, Springer Science & Business Media, 2011.
3. BRAGG, Network Security: The Complete Reference, McGraw Hill Professional, 2012.

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes	RBT Level*
01	Understand the concept of secure operating system & virtualization	UN
02	Compare various security features in Multics, Windows and Linux OS.	UN
03	Analyze different models for securing commercial OS	AN
04	Differentiate the System Management Mode (SMM), chip-set architecture	AN
05	Critiquing how the BIOS interacts with the Trusted Platform Module (TPM) and the measured boot process	EV

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Suggested Course Practical List:

- The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required:

- Course-related online MOOCs on NPTEL/SWAYAM platform
- Tools: GnuPG, TrueCrypt, Application security, Host security
- OWASP
- Pentester Online Academy platform
- Recently Published papers/articles in reputed journals