uc3m | Universidad Carlos III de Madrid

COURSE: Cyber Defense Systems		
MÁSTER: Master in Cybersecurity	**YEAR: 1st**	**TERM: 1st**

WEEKLY SCHEDULE OF THE COURSE

WEEK	SESSION	DESCRIPTION OF THE SESSION	GROUP (mark with X)		SPECIAL ROOM FOR SESSION (Computer class room, audio-visual classroom)	Indicate YES/NO if the session requires 2 teachers	WEEKLY WORK FOR STUDENT		
			LECTURES	SEMINARS			DESCRIPTION	CLASS HOURS	HOMEWORK HOURS (Max. 7h per week)
1	1	**Course overview** **Introduction to Cyberdefense**	X				Review the concepts learned in session 1. Complete all mini-lab tasks, if necessary. Prepare sessions 3 and 4.	1,66	4
	2	**Mini-lab: Configuration of virtual environment**		X	Lab.			1,66	
2	3	**Local sensors: Audit and analysis of events (I)**: Introduction to local sensors **Mini-lab: Rsyslog**		X	Lab.		Review the concepts learned in sessions 3 and 4. Complete all mini-labs tasks, if necessary. Prepare sessions 5 and mini-lab	1,66	4
	4	**Local sensors: Audit and analysis of events (II)**: Management of users and accesses **Mini-lab: User management**		X	Lab.			1,66	
3	5	**Local sensors: Audit and analysis of events (III)**: Analysis of security logs **Mini-lab: Log rotation**		X	Lab.		Review the concepts learned in session 5. Complete all mini-lab tasks, if necessary. Prepare sessions 7 and 8.	1,66	4
	6	**Mini-lab: Log configuration**		X	Lab.			1,66	
4	7	**Firewalls and network segmentation (I)**: Fundamentals of traffic filtering	X				Review the concepts learned in sessions 7 and 8. Prepare session 9.	1,66	3
	8	**Firewalls and network segmentation (II)**: Types of firewalls	X					1,66	

5	9	**Firewalls and network segmentation (III)**: Network segmentation	X				Review the concepts learned in session 9. Complete all mini-lab tasks, if necessary. Prepare laboratory	1,66	4
	10	**Mini-lab: iptables**		X	Lab.			1,66	
6	11	**Firewalls laboratory (I)**		X	Lab.	Yes	Complete all laboratory tasks, if necessary. Edit laboratory deliverable. Prepare sessions 13 and 14.	1,66	7
	12	**Firewalls laboratory (II)**		X	Lab.	Yes		1,66	
7	13	**Intrusion Detection and Prevention (I)**: Signature detection	X				Review the concepts learned in sessions 13 and 14. Prepare session 15.	1,66	3
	14	**Intrusion Detection and Prevention (II)**: Anomaly detection	X					1,66	
8	15	**Intrusion Detection and Prevention (III)**: Automated response to intrusion attacks	X				Review the concepts learned in session 15. Complete all mini-lab tasks, if necessary. Prepare laboratory	1,66	4
	16	**Mini-lab: Snort**		X	Lab.			1,66	
9	17	**IDS/IPS laboratory (I)**		X	Lab.	Yes	Complete all laboratory tasks, if necessary. Edit laboratory deliverable. Prepare sessions 19 and 20.	1,66	7
	18	**IDS/IPS laboratory (II)**		X	Lab.	Yes		1,66	
10	19	**Security Information and Event Management (SIEM) (I)**: Introduction and SIEMs architectures	X				Review the concepts learned in sessions 19 and 20. Prepare sessions 21 and 22	1,66	3
	20	**Security Information and Event Management (SIEM) (II)**: Aggregation and correlation rules	X					1,66	
11	21	**Security Information and Event Management (SIEM) (III)**: Intrusion detection networks **Mini-lab: OSSIM**		X	Lab.		Review the concepts learned in sessions 21 and 22. Complete all mini-labs tasks, if necessary. Prepare laboratory	1,66	4
	22	**Security Information and Event Management (SIEM) (IV)**: Strategies for network sensing **Mini-lab: Log normalisation**		X	Lab.			1,66	
12	23	**SIEM Laboratory (I)**		X	Lab.	Yes	Complete all laboratory tasks, if necessary. Edit laboratory deliverable. Prepare final exam.	1,66	7
	24	**SIEM Laboratory (II)**		X	Lab.	Yes		1,66	
							57	**40**	**54**

TOTAL *(Total 1 + Total 2. Max 180 hours)*	**94**