School of Government

LUISS

1. Detailed Syllabus of Module A

Module A consists of seven (7) sessions:

Session ID	Name of the Session	Hrs
A.1	Operating systems	25
A.2	Internet	12
A.3	Application protocols and internet-based services	18
A.4	Information systems	18
A.5	Fundamental Concepts of Programming	30
A.6	Introduction to Database Systems	30
A.7	Programming Languages	138

a. Syllabus of Session A.1

The Session A.1 “Operating systems” introduces the fundamentals of modern Windows and Linux operating systems including user and kernel space, virtual memory and file systems.
This course covers the basics of operating systems. It describes the underlying theory and the architectural solutions of modern operating systems by focusing on multitasking, virtual memory and file system management for Windows and Linux operating systems.
It introduces also the use of a shell (BASH, Command prompt), and of scripting. Moreover, it describes the main management techniques for operating system configuration, software management, resource monitoring, troubleshooting. The module “Internet” focuses on the basics of the TCP/IP communication stack and of its most important protocols such as Ethernet, ARP, IP, ICMP, TCP, UDP.
This Session provides the basic knowledge related to modern computer networks. Moreover, the course focuses on the main instruments provided by Linux and Windows for configuring, monitoring and diagnosing each protocol.

b. Syllabus of Session A.2

Session A.2 provides trainees with the basic knowledge related to modern computer networks, introducing the TCP/IP network stack and the different protocols for host-to-network, network and transport levels. It also focuses on the main tools of Linux and Windows to configure, monitor and diagnose each protocol

c. Syllabus of Session A.3

The session A.3 describes the main services provided through the Internet. It focuses on the client/server paradigm, on the main network services and of the related protocols. It shows to the trainees the client/server paradigm on the main network services and of the related protocols, since applications and Internet surfing happens through them

d. Syllabus of Session A.4

Session A.4 provides trainees with the knowledge of the main architectures for Web-based and locally distributed systems, focusing on the principal components of a multi-tier Web architecture (front-end, Application Server, Database Management System) and their interactions.
It also shows the typical architectural solutions of modern data centres and geographically distributed services. Moreover, it presents the typical architectural solutions of modern data centres and geographically distributed services, such as Google and Cloud.

e. Syllabus of Session A.5

Session A.5 introduces the fundamental concepts of procedural programming.
It provides trainees with a series of tools and methodologies at the base of programming such as data types, control structures, functions, arrays, files, and the mechanics of running, testing, and debugging.

f. Syllabus of Session A.6

Session A.6 shows to the trainees the main concepts of database management. Indeed, databases are a necessary technology for the modern organizations by now, for this reason it is important to have an in-depth know of its principal features.

g. Syllabus of Session A.7

Session A.7 provides a wide knowledge to manage PHP (Personal Home Page), that is a server-side scripting language necessary to design and develop dynamic web pages based on database. It is open source, for this reason it is important to be able to manage it. It also shows the main features and uses of MySQL and of a mobile programming language (i.e. in general the differences among different used programming languages such as SWIFT/JAVA/PYTHON/PEARL and the reasons of their differences).

2. Detailed Syllabus of Module B

Module B consists of eleven (11) sessions:

Session ID	Name of the Session	Hrs
B.1	Cyber Security Risk Assessment & Management	36
B.2	Applications of hashing and cryptography	24
B.3	Authentication and authorization systems	24
B.4	Client and server hardening (Windows and Linux)	24
B.5	Design of secure architectures for wired and wireless networks	24
B.6	Secure Internet communications	24
B.7	Software security	24
B.8	Mobile device management	24
B.9	Logging, monitoring and event management systems (SIEM)	24
B.10	Incident management	34
B.11	Security management	60
	Final Thesis	9

a. Syllabus of Session B.1

Session B.1 shows to the trainees the general information security risk management framework and its practices and the best way to identify and model information security risks and to apply both qualitative and quantitative risk assessment methods. It also equips trainees with the practical knowledge to develop a cyber security risk management strategy that delivers the required outcomes in their organization.

b. Syllabus of Session B.2

Session B.2 provides trainees with knowledge about the main applications of modern cryptographic and hashing techniques in the field of computer and communication security. It shows the underlying mechanisms of digital signatures, digital certificates and certification authorities. It also introduces the main protocols used to implement Virtual Private Networks, secure interactions with Web servers and e-mail security.

c. Syllabus of Session B.3

Session B.3 provides trainees with knowledge about the main modern authentication and authorization techniques and the latest methodologies for the management of digital identities. It supplies basic knowledge and skills for the design, deployment, configuration and management of authentication and authorization systems for complex information systems. It also shows state-of-the-art tools and solutions for Windows and Linux operating systems. In addition, it introduces innovative authentication and authorization systems deployed in distributed systems.

d. Syllabus of Session B.4

Session B.4 provides trainees with knowledge of the theory and the main practices to harden Windows- and Linux-based systems. It also shows configuration and management best practices and the main countermeasures that address known vulnerabilities and make it harder for an attacker to mount a successful attack.

e. Syllabus of Session B.5

Session B.5 provides trainees with knowledge about tools and techniques to design and implement secure communication solutions for the main geographically distributed systems and networks. It also shows solutions for the implementation of VPNs to guarantee authentication and confidentiality over untrusted networks. In addition, it presents the main protocols that increase security for several internet services.

f. Syllabus of Session B.6

Session B.6 provides trainees with the knowledge about the main tools and techniques to increase security in LAN. In particular, it shows the use of segmentation, monitoring, VLAN, firewall, DMZ, NAT, intrusion detection and prevention systems. In addition, it describes the design of secure wireless networks based on IEEE 802.11 protocols, analysing the main protocols for wireless authentication and cryptography: WPA2 and the obsolete WEP and WPA.

g. Syllabus of Session B.7

Session B.7 provides trainees with the knowledge about the tools and of the techniques needed to design and implement log management systems based on the centralization of logs and monitoring information when generated by remote hosts. This is to facilitate log analysis and guarantee log integrity even if hosts generating logs are compromised. It also shows security requirements for log management systems (that handle log files generated by critical systems and applications) and for the certification of log integrity. In addition, it describes the state of the art for Security Information and Event Management (SIEM) that allows the integration of data generated by distributed and hybrid intrusion detection systems, log centralization systems, alarm and video surveillance and other heterogeneous information sources.

h. Syllabus of Session B.8

Session B.8 provides trainees with knowledge of the main techniques to increase software security, especially for software that is remotely accessible through Internet. It also shows the main countermeasures to correct known software vulnerabilities and mitigate known and unknown software vulnerabilities, improving configurations and platforms.

i. Syllabus of Session B.9

Session B.9 provides trainees with knowledge about the technologies and of the products necessary to improve the security of mobile applications and the protection of enterprise sensitive data describing also the main policies. Indeed, the large diffusion of mobile devices for personal and business goals is introducing new issues for the protection of their data. For this reason, this module shows the best solutions for centralized management of the main mobile devices, highlighting procedures to enforce authentication mechanisms, secure voice and data communications, limitation to the type of applications, software integrity verification, data encryption, remote data deletion, position tracking, and other important countermeasures.

j. Syllabus of Session B.10

Session B.10 deals with the Incident management, that is the ability to prepare for and respond to events that present a negative effect to a network and it is considered the next level of incident response. This course teaches how to respond to a network security incident and how it is useful manage data from past incidents to strengthen their defences. It provides students the most important skills and techniques required for managing an incident effectively by Security Operations Centre (SOC), ensuring that it is successfully and timely resolved.

k. Syllabus of Session B.11

Session B.11 illustrates methodologies and standards that should be pursued in the design, implementation and assessment of secure systems and services.

The systemic view of the security engineering process proposed in this module allows trainees to integrate and organize the overall information presented in the other modules of the Cyber defence course.

Furthermore, has two objectives:

The former is to provide all information required to assess the risk related to networked computer systems, and to plan improvements and investments.

The latter is to show the most important standards for security management, with a specific focus on ISO27001 and ITIL.

3. Detailed Syllabus of Module C

Module C consists of five (5) sessions:

Session ID	Name of the Session	Hrs
C.1	System Vulnerability Assessment	30
C.2	System Penetration Test	30
C.3	Application Vulnerability Assessment	30
C.4	Application Penetration Test	30
C.5	Introduction to Malware Reverse Engineering	42

a. Syllabus of Session C.1

Session C.1 provides trainees with a methodology to identify main system vulnerabilities, starting from Information Gathering activities. This module will be also based on hands-on labs on tools for Information Gathering phase and Vulnerability scanning.

b. Syllabus of Session C.2

Session C.2 provides trainees with the knowledge of exploitation techniques of system vulnerabilities in different kind of infrastructures. The module will be also based on hands-on labs related to real case studies attacks at the Infrastructure level.

c. Syllabus of Session C.3

Session C.3 provides trainees with knowledge of web-based application vulnerabilities and their countermeasures. This module provides an in-depth methodology regarding protection of applications based on real case studies.

d. Syllabus of Session C.4

Session C.4 provides trainees with the knowledge of techniques related to real attacks that could be performed on multiple web-based application. The module will be also based on hands-on labs related to the use of tools to exploit vulnerabilities at the Application layer.

e. Syllabus of Session C.5

Session C.5 provides trainees with an introduction of the topic related to Reverse Engineering Malwares. It regards the capability to know and identify the different stages of a malware and how to analyse it using static and live analysis inside a laboratory.