



INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA ACADÉMICA

DIRECCIÓN DE EDUCACIÓN SUPERIOR

SYNTHESIZED SCHOOL PROGRAM



ACADEMIC UNIT: Escuela Superior de Cómputo
ACADEMIC PROGRAM: Ingeniería en Sistemas Computacionales.
LEARNING UNIT: Advanced Computing Systems Programming **LEVEL:** III

AIM OF THE LEARNING UNIT:

The student develops computer networks security systems based on available infrastructure, connectivity devices, tools and security policies.

CONTENTS:

- I. Network Security.
- II. Managing Network Security.
- III. Monitoring and Security Architectures.
- IV. Intrusion Attacks.
- V. Denial of Service.
- VI. Data Theft Attack.

TEACHING PRINCIPLES:

A project-oriented learning strategy will be applied. The teacher will lead the course with the heuristic method, for which several techniques will be implemented as: case studies, documentary research, conducting worksheets, guided discussion, teamwork, presentation of issues and development practices.

EVALUATION AND PASSING REQUIREMENTS:

The program will evaluate the students in a continuous formative and summative way, which will lead into the completion of project portfolio. Some other assessing methods will be used, such as revisions, practical's, class participation, exercises, learning evidences and a final project.

Other means to pass this Unit of Learning:

- Evaluation of acknowledges previously acquired, with base in the issues defined by the academy.
- Official recognition by either another IPN Academic Unit of the IPN or by a national or international external academic institution besides IPN.

REFERENCES:

- Cole, E. Krutz, R. Conley, J. (2009), *Network Security Bible 2nd Edition*, USA: John Wiley & Sons. ISBN: 978-0-470-50249-5.
- Gómez, A. (2007), *Enciclopedia de la Seguridad Informática*, España: Alfa Omega. ISBN 9701512661
- Long J. (2005), *Google Hacking for Penetration Testers*, USA: Syngress, ISBN: 1-931836-36-1
- Mirkovic, J. Dietrich, S. Dittrich, D. Reiher, P. (2005), *Internet Denial of Service: Attack and Defense Mechanisms*, USA: Prentice Hall. ISBN-13: 9780131475731
- Stallings, W. (2004), *Fundamentos de Seguridad en Redes*, España: Pearson, ISBN 8420540021



INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR



ACADEMIC UNIT: Escuela Superior de Cómputo.
ACADEMIC PROGRAM: Ingeniería en Sistemas Computacionales
LATERAL OUTPUT: Analista Programador de Sistemas de Información.
FORMATION AREA: Professional.
MODALITY: Presence.

LEARNING UNIT: Advanced Computing Systems Programming.
TYPE OF LEARNING UNIT: Theoretical - Practical, Optative.
VALIDITY: August, 2011.
LEVEL: III.
CREDITS: 7.5 Tepic, 4.38 SATCA

ACADEMIC AIM

This learning unit contributes to the profile of graduated of Ingeniería en Sistemas Computacionales, developing the skills of abstraction, analysis and design of computer network security.

Design and Implementation of management systems for network security and monitoring using the architectures, protocols and standards exist. It also develops strategic thinking, creative thinking, collaborative and participatory and assertive communication.

Required of learning units Algoritmia y Programación Estructurada, Sistemas Operativos, así como de Redes de Computadoras, Aplicaciones para Comunicaciones en Red y Administración de Servicios de Red.

AIM OF THE LEARNING UNIT:

The student develops computer networks security systems based on available infrastructure, connectivity devices, tools and security policies.

CREDITS HOURS

THEORETICAL CREDITS / WEEK: 3.0

PRACTICAL CREDITS / WEEK: 1.5

THEORETICAL HOURS / SEMESTER: 54

PRACTICAL HOURS / SEMESTER: 27

AUTONOMOUS LEARNING HOURS: 54

CREDITS HOURS / SEMESTER: 81

LEARNING UNIT DESIGNED BY:
Academia de Sistemas Distribuidos.

REVISED BY:
Dr. Flavio Arturo Sánchez Garfias.
Subdirección Académica

APPROVED BY:
Ing. Apolinar Francisco Cruz Lázaro.
Presidente del CTCE

AUTHORIZED BY: Comisión de Programas Académicos del Consejo General Consultivo del IPN

Ing. Rodrigo de Jesús Serrano Domínguez
Secretario Técnico de la Comisión de Programas Académicos



INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR



LEARNING UNIT: Advanced Computing Systems Programming

PAGE: 3 **OUT OF** 12

THEMATIC UNIT: I			TITLE: Network Security			
UNIT OF COMPETENCE						
The student develops a proposal security of a computer network, based on requirements and resources available.						
No.	CONTENTS	Teacher led-instruction HOURS		Autonomous Learning HOURS		REFERENCES KEY
		T	P	T	P	
1.1	What is network security?	0.5		1.0		2B, 5B
1.2	Risk types	0.5		1.0		
1.3	Attack types		0.5	1.0	1.0	
1.4	Type of attackers			0.5		
1.5	Study cases relating to security		0.5	1.0	1.0	
1.6	Ethic and commitment in security	1.0				
1.7	Security services and mechanisms			1.0		
1.8	Network security models	0.5		1.0		
	Subtotal:	2.5	1.0	6.5	2.0	
TEACHING PRINCIPLES						
This unit will be addressed using learning strategy and project-oriented heuristics, enabling the consolidation of the following learning techniques: documentary inquiry, guided discussion, case studies, problem solving, exhibition of complementary topics and practical work.						
LEARNING EVALUATION						
Diagnostic Evaluation						
Project Portfolio:						
Evaluation of individual research		5%				
Research Worksheets		5%				
Report of practicals		30%				
Project Proposal		5%				
Self-assessment rubrics		2.5%				
Co-evaluation rubrics		2.5%				
Evidence of learning		50%				



INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR



LEARNING UNIT: Advanced Computing Systems Programming

PAGE: 4 OUT OF 12

THEMATIC UNIT: II		TITLE: Managing Network Security				
UNIT OF COMPETENCE						
The student applies security policies and strategies to the project, based on its requirements and mechanisms for responding to security incidents.						
No.	CONTENTS	Teacher led-instruction HOURS		Autonomous Learning HOURS		REFERENCES KEY
		T	P	T	P	
2.1	Security strategies	1.0	0.5	1.0	1.0	2B, 6B
2.2	Security policies	1.0		1.0		
2.3	Security monitoring					
2.4	Deployment mechanisms	0.5	1.0			
2.5	Maintaining security	1.0	1.0			
2.6	Security incident response		0.5	1.0	1.0	
Subtotal:		3.5	1.0	7.0	2.0	
TEACHING PRINCIPLES						
This unit will be addressed using learning strategy and project-oriented heuristics, enabling the consolidation of the following learning techniques: documentary inquiry, guided discussion, case studies, problem solving, exhibition of complementary topics and practical work.						
LEARNING EVALUATION						
Project Portfolio:						
Worksheets		5%				
Report of practicals		25%				
Project report (diagram and equipment configuration)		15%				
Self-assessment rubrics		2.5%				
Co-evaluation rubrics		2.5%				
Evidence of learning		50%				



INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR



LEARNING UNIT:

Advanced Computing Systems Programming

PAGE: 5

OUT OF 12

THEMATIC UNIT: III

TITLE: Monitoring and Security Architectures

UNIT OF COMPETENCE

The student designs network architecture based on settings such as firewalls, intrusion detection systems, virtual private networks and monitoring tools.

No.	CONTENTS	Teacher led-instruction HOURS		Autonomous Learning HOURS		REFERENCES KEY
		T	P	T	P	
3.1	Monitoring for network security	0.5		1.0		7B, 8B
3.2	Monitoring for detection and its limitations	1.0		0.5		
3.3	Applications for network monitoring		0.5	0.5	1.0	
3.4	Operations for the security process in monitoring		0.5	0.5	1.0	
3.5	Security architecture using firewalls	0.5		1.0		
3.6	Security architecture using IDS		1.5	1.0	1.5	
3.7	Security architecture using VPNs	0.5		1.0		
Subtotal:		2.5	2.5	5.5	3.5	

TEACHING PRINCIPLES

This unit will be addressed using learning strategy and project-oriented heuristics, enabling the consolidation of the following learning techniques: documentary inquiry, guided discussion, case studies, problem solving, exhibition of complementary topics and practical work.

LEARNING EVALUATION

Project Portfolio:

Worksheets	5%
Report of practicals	20%
Project report (diagram and equipment configuration)	20%
Self-assessment rubrics	2.5%
Co-evaluation rubrics	2.5%
Evidence of learning	50%

THEMATIC UNIT: IV				TITLE: Intrusion Attacks			
UNIT OF COMPETENCE							
The student designs a set of rules for an intrusion detection system unsecured network, based on case studies.							
No.	CONTENTS	Teacher led-instruction HOURS		Autonomous Learning HOURS		REFERENCES KEY	
		T	P	T	P		
4.1	Anatomy of intrusion attacks	0.5		1.0		1B, 3C	
4.2	Obtaining information about network to attack.		0.5	1.0	1.0		
4.3	Determination of operating system		1.0	0.5	0.5		
4.4	Determination of services	0.5		1.0			
4.5	Discovering DNS	0.5		1.0			
4.6	Mechanisms to detect an intrusion attack		0.5	1.0	1.0		
4.7	Mechanisms to prevent intrusion attacks		1.5	1.0	0.5		
	Subtotal:	1.5	3.0	6.5	3.0		
TEACHING PRINCIPLES							
This unit will be addressed using learning strategy and project-oriented heuristics, enabling the consolidation of the following learning techniques: documentary inquiry, guided discussion, case studies, problem solving, exhibition of complementary topics and practical work.							
LEARNING EVALUATION							
Project Portfolio:							
Worksheets		5%					
Report of practicals		15%					
Heading the project implementation and progress		25%					
Self-assessment rubrics		2.5%					
Co-evaluation rubrics		2.5%					
Evidence of learning		50%					



INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR



LEARNING UNIT: Advanced Computing Systems Programming

PAGE: 8 **OUT OF** 12

THEMATIC UNIT: VI				TITLE: Data Theft Attack		
UNIT OF COMPETENCE						
The student sets up systems to prevent and detect data theft attacks, based on vulnerability assessment tools and detection of anomalies						
No.	CONTENTS	Teacher led-instruction HOURS		Autonomous Learning HOURS		REFERENCES KEY
		T	P	T	P	
6.1	Types of data theft attacks	0.5		1.0		13B, 12C
6.2	Anatomy of data theft attacks	0.5		1.0		
6.3	Power Session Data	0.5	0.5	1.0	1.0	
6.4	Packet Analysis	0.5	0.5	0.5	1.0	
6.5	Attack detection mechanisms of information theft	0.5	0.5	0.5	1.0	
6.6	Mechanisms to prevent data theft attack	0.5	0.5	1.0	1.0	
	Subtotals:	3.0	2.0	5.0	4.0	
TEACHING PRINCIPLES						
This unit will be addressed using learning strategy and project-oriented heuristics, enabling the consolidation of the following learning techniques: documentary inquiry, guided discussion, case studies, problem solving, exposure of your project team and practical work.						
LEARNING EVALUATION						
Project Portfolio:						
Presenting the team final		15%				
Report of practicals		15%				
Report and project delivery		35%				
Self-assessment rubrics		2.5%				
Co-evaluation rubrics		2.5%				
Evidence of learning		30%				



INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR



LEARNING UNIT: Advanced Computing Systems Programming

PAGE: 9 OUT OF 12

RECORD OF PRACTICALS

No.	NAME OF THE PRACTICAL	THEMATIC UNITS	DURATION	ACCOMPLISHMENT LOCATION
1	Detection of computers configured in promiscuous mode.	I	1.5	Salas de cómputo de la escuela
2	DNS poisoning	I	1.5	
3	Configure firewalls.	II	1.5	
4	Setting up a communication device to respond to security alerts	II	1.5	
5	Configuring an IDS	III	3.0	
6	Setting up a monitoring area	III	3.0	
7	Scanning a network and determining the computer's operating system.	IV	3.0	
8	Setting up a honeypot	IV	3.0	
9	Attack login	V	3.0	
10	Obtaining information from a user-FTP	VI	1.5	
11	Forensic analysis of a committed team	VI	3.0	
12	Setting up a VPN server	VI	1.5	
		TOTAL OF HOURS	27.0	

EVALUATION AND PASSING REQUIREMENTS:

Practices contributing 30% to the calification in in Unit I.
Practices contributing 25% to the calification in in Unit II.
Practices contributing 20% to the calification in in Unit III.
Practices contributing 15% to the calification in in Unit IV, V and VI.

Practices are considered mandatory to pass this learning unit.



INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR



LEARNING UNIT:

Advanced Computing Systems Programming

PAGE: 10 OUT OF 12

PERIOD	UNIT	EVALUATION TERMS
1	I y II	Continuous evaluation 50% and written learning evidence 50%
2	III y IV	Continuous evaluation 50% and written learning evidence 50%
3	V	Continuous evaluation 50% and written learning evidence 50%
	VI	Continuous evaluation 70% and written learning evidence 30%
		<p>The learning unit I and II are 30% worth of the final score The learning unit III and IV are 30% worth of the final score The learning unit V is 20% worth of the final score The learning unit VI is 20% worth of the final score</p> <p>Other means to pass this Learning Unit:</p> <ul style="list-style-type: none">• Evaluation of acknowledges previously acquired, with base in the issues defined by the academy.• Official recognition by either another IPN Academic Unit of the IPN or by a national or international external academic institution besides IPN. <p>If accredited by Special Assessment or a certificate of proficiency, this will be based on guidelines established by the academy on a previous meeting for this purpose.</p>



INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR



LEARNING UNIT:

Advanced Computing Systems Programming

PAGE: 11 OUT OF 12

KEY	B	C	REFERENCES
1	X		Cole, E. (2002), <i>Hackers Beware</i> , USA: Sams Publishing, ISBN: 0735710090
2	X		Cole, E. Krutz, R. Conley, J. (2009), <i>Network Security Bible 2nd Edition</i> , USA: John Wiley & Sons. ISBN: 978-0-470-50249-5.
3		X	Conway, R. Cordingley, J. (2004), <i>Code Hacking: A Developer's Guide to Network Security, Volumen 1</i> , USA: Charles River Media, ISBN: 1584503149
4		X	Chirillo, J. (2001), <i>Hack Attacks Revealed: A Complete Reference with Custom Security Hacking Toolkit</i> , USA: Wiley, ISBN: 047141624X
5	X		EC-Council. (2009), <i>Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems</i> , USA: Cengage Learning, ISBN: 1435483642
6	X		Gómez, A. (2007), <i>Enciclopedia de la Seguridad Informática</i> , España: Alfa Omega. ISBN 9701512661
7	X		Gregg, M. (2008), <i>Build Your Own Security Lab: A Field Guide for Network Testing</i> , USA: John Wiley and Sons, ISBN: 0470179864
8	X		Gregg, M. (2006), <i>Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network</i> , USA: Syngress, ISBN: 1597491098
9		X	Long J. (2005), <i>Google Hacking for Penetration Testers</i> , USA: Syngress, ISBN: 1-931836-36-1
10		X	Mirkovic, J. Dietrich, S. Dittrich, D. Reiher, P. (2005), <i>Internet Denial of Service: Attack and Defense Mechanisms</i> , USA: Prentice Hall. ISBN-13: 9780131475731
11	X		Stallings, W. (2004), <i>Fundamentos de Seguridad en Redes</i> , España: Pearson, ISBN 8420540021
12		X	Russell, R. Mirza A., D. (2002), <i>Hack Proofing your Network</i> , USA: Syngress, ISBN: 1928994709
13	X		Russell, R. (2003), <i>Stealing the Network: How to Own the Box</i> , USA: Syngress, ISBN: 1931836876



INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA ACADÉMICA

DIRECCIÓN DE EDUCACIÓN SUPERIOR



TEACHER EDUCATIONAL PROFILE PER LEARNING UNIT

1. GENERAL INFORMATION

ACADEMIC UNIT: Escuela Superior de Cómputo.

ACADEMIC PROGRAM: Ingeniería en Sistemas Computacionales.

LEVEL III

FORMATION AREA:

Institutional	Basic Scientific	Professional	Terminal and Integration
---------------	------------------	--------------	--------------------------

ACADEMY: Sistemas Distribuidos.

LEARNING UNIT: Advanced Computing Systems Programming.

SPECIALTY AND ACADEMIC REQUIRED LEVEL: Masters Degree or network security specialist.

2. AIM OF THE LEARNING UNIT:

The student develops computer networks security systems based on available infrastructure, connectivity devices, tools and security policies.

3. PROFESSOR EDUCATIONAL PROFILE:

KNOWLEDGE	PROFESSIONAL EXPERIENCE	ABILITIES	APTITUDES
<ul style="list-style-type: none">Architecture TCP / IPAnalysis of protocols and programmingComputer Network SecurityMonitoring of Computer Networks	<ul style="list-style-type: none">Experience in computer network securityExperience using applications for security and network monitoringExperience in safety equipment configuration: firewalls, IDS and VPNs.Experience managing a programming language	<ul style="list-style-type: none">Ability to communicate well orally and in writing.Ability to review software code and find errors.Easy management of groups.Management of teaching methods focused on learning	<ul style="list-style-type: none">Architecture TCP / IPAnalysis of protocols and programmingComputer Network SecurityMonitoring of Computer Networks

DESIGNED BY

REVISED BY

AUTHORIZED BY

Ing. Gilberto Sánchez Quintanilla
COORDINATING PROFESOR

Dr. Flavio Arturo Sánchez Garfias
Subdirector Académico

Ing. Apolinar Francisco Cruz Lázaro
Director

Ing. Eduardo Gutiérrez Aldana
COLLABORATING PROFESSORS

Date: 2011