

# Testi del Syllabus

Resp. Did.	<b>VELTRI LUCA</b>	<b>Matricola: 006125</b>
Docente	<b>VELTRI LUCA, 3 CFU</b>	
Anno offerta:	<b>2016/2017</b>	
Insegnamento:	<b>1005261 - NETWORK SECURITY + LABORATORY (UNIT 2)</b>	
Corso di studio:	<b>5052 - COMMUNICATION ENGINEERING - INGEGNERIA DELLE TELECOMUNICAZIONI</b>	
Anno regolamento:	<b>2016</b>	
CFU:	<b>3</b>	
Settore:	<b>NN</b>	
Tipo Attività:	<b>F - Caratterizzante</b>	
Anno corso:	<b>1</b>	
Periodo:	<b>Secondo Semestre</b>	
Sede:	<b>PARMA</b>	



## Testi in italiano

<b>Lingua insegnamento</b>	Inglese
<b>Contenuti</b>	Esercitazioni in laboratorio su: <ul style="list-style-type: none"><li>- Certificati digitali X.509, CA, applicazioni (e.g. HTTPS), PGP;</li><li>- IPSec, TLS;</li><li>- Protocol analyzer, Network scanning, Vulnerability test;</li><li>- Firewall (Linux netfilter).</li></ul>
<b>Testi di riferimento</b>	L. Veltri, "Network Security", Lucidi del corso
<b>Obiettivi formativi</b>	<p>L'obiettivo di questa parte è fornire allo studente alcune conoscenze pratiche su alcuni strumenti per la sicurezza e mettere in pratica alcuni dei concetti e meccanismi visti nel corso di Sicurezza nelle reti.</p> <p>Le capacità di applicare le conoscenze e comprensione elencate risultano essere in particolare:</p> <ul style="list-style-type: none"><li>- maneggiare strumenti per la crittografia, firma digitale, generazione e utilizzare certificati digitali X.509 e PGP;</li><li>- configurare e utilizzare protocolli per comunicazioni sicure, quali ad esempio IPSec e TLS;</li><li>- utilizzare strumenti per il monitoraggio di una rete, enumerazione delle risorse e scansione delle possibili vulnerabilità;</li><li>- configurare firewall in ambiente unix/linux.</li></ul>
<b>Prerequisiti</b>	Corso di Sicurezza nelle reti
<b>Metodi didattici</b>	Attività di laboratorio (21h)

<b>Modalità di verifica dell'apprendimento</b>	Auto verifica. Sviluppo di un progetto.
<b>Programma esteso</b>	Vedi descrizione in inglese



## Testi in inglese

<b>Lingua insegnamento</b>	English
<b>Contenuti</b>	Laboratory activities on: <ul style="list-style-type: none"> <li>- Creation and use of digital certificates (X.509), CA, applications, PGP;</li> <li>- IPSec, TLS;</li> <li>- Protocol analyzer, Network scanning, Vulnerability test;</li> <li>- Firewall (Linux netfilter).</li> </ul>
<b>Testi di riferimento</b>	L. Veltri, "Network Security", Slides of the course
<b>Obiettivi formativi</b>	<p>The objective of this part is to provide the student with practical knowledge of some security tools, and to practically use concepts and mechanisms encountered within the course of Network Security.</p> <p>Applying knowledge and understanding are:</p> <ul style="list-style-type: none"> <li>- use of tools for cryptography, digital signature, creation and managing of digital certificates X.509 and PGP;</li> <li>- configuring and use of protocols for secure communications, such as IPSec and TLS;</li> <li>- use of tools for network monitoring, resources enumeration, and vulnerabilities scanning;</li> <li>- configuring firewalls under unix/linux OS.</li> </ul>
<b>Prerequisiti</b>	Network security course
<b>Metodi didattici</b>	Laboratory activities (21h)
<b>Modalità di verifica dell'apprendimento</b>	Self verification. Project development.
<b>Programma esteso</b>	<p>Syllabus (every laboratory activity = 2 hours)</p> <p>Laboratory activity 1: cryptography functions (with openssl)</p> <p>Laboratory activity 2: X.509 certificates and certification authority (CA)</p> <p>Laboratory activity 3: network sniffing; MITM attack; vulnerability scanning</p> <p>Laboratory activity 4: linux firewall: netfilter and iptables</p> <p>Project assignment</p>