Testi del Syllabus

Resp. Did.	**BARTOLI Alberto**	Matricola:	**005943**

Anno offerta:	**2016/2017**
Insegnamento:	**216MI - RETI DI CALCOLATORI II E PRINCIPI DI SICUREZZA INFORMATICA**
Corso di studio:	**IN20 - INGEGNERIA ELETTRONICA E INFORMATICA**
Anno regolamento:	**2016**
CFU:	**9**
Settore:	**ING-INF/05**
Tipo Attività:	**B - Caratterizzante**
Anno corso:	**1**
Periodo:	**Secondo Semestre**

Testi in italiano

Lingua insegnamento	Italiano
Contenuti (Dipl.Sup.)	Implementazione di TCP Tecnologie per l'accesso ad Internet con indirizzi privati (NAT/NAPT) Attacchi a TCP. Modelli di attacco informatico. Autenticazione. Attacchi a database di password. Kerberos VPN Tecnologie per Single Sign On su scala locale e su scala geografica Tecnologie per SSO, delega di autenticazione ed autorizzazione su scala geografica, identity federation: OAuth 2; OpenID Connect; SAML Protected Wi-Fi Attacchi informatici: modalità e motivazioni Web security Denial of service
Obiettivi formativi	Il corso presenta le principali tecnologie delle reti di calcolatori ormai divenute essenziali in ogni dominio applicativo ICT: smart cities, home automation, automotive, distribuzione dell'energia, automazione industriale, reti di sensori, trasporti intelligenti, e-government e così via. L'analisi è focalizzata in modo particolare sui problemi di sicurezza, divenuti ormai di importanza fondamentale in ogni contesto applicativo.
Prerequisiti	Il corso presuppone la conoscenza degli argomenti trattati in Reti di Calcolatori I.
Altre informazioni	Vedi http://bartoli.inginf.units.it (sezione didattica)
Modalità di verifica dell'apprendimento	Esame scritto su problemi basati su scenari applicativi reali, seguito da interrogazione orale.

Programma esteso	Implementazione di TCP Tecnologie per l'accesso ad Internet con indirizzi privati (NAT/NAPT) Attacchi a TCP. Modelli di attacco informatico. Autenticazione. Protocolli APOP, NTLM. Attacchi a database di password. Password salting. Kerberos: funzionalità di autenticazione mutua, riservatezza, delega di autenticazione su scala locale. Implementazione. Autenticazione e riservatezza in PPP. Tunnel PPP. VPN: applicazioni ed implementazione basata su SSL. Tecnologie per Single Sign On su scala locale. LDAP, Kerberos. Tecnologie per SSO, delega di autenticazione ed autorizzazione su scala geografica, identity federation: OAuth 2; OpenID Connect; SAML Protected Wi-Fi: WPA Personal e WPA Enterprise. Malvertising e botnet Vulnerabilità e mercati 0-day Web security: attacchi man-in-the-middle ad HTTPS; Strict Transport Security, Public Key Pinning, Cross- Site Request Forgery, Cross-Site Scripting Denial of service: modalità di attacco e di difesa

Testi in inglese

Lingua insegnamento	Italian
Contenuti (Dipl.Sup.)	TCP Implementation Technologies for Internet access based on private addressing (NAT/NAPT) TCP attacks. Attack models Authentication Attacks on password databases Kerberos VPN Single Sign On technologies for local deployment and geographic deployment OAuth 2; OpenID Connect; SAML Protected Wi-Fi Web security Denial of service
Obiettivi formativi	This course illustrates the main computer network technologies which have become essential in every ICT-based application domain: smart cities, home automation, automotive, energy distribution, industrial automation, sensor networks, intelligent transportation, e-government and so on. The analysis places special emphasis on security problems, whose importance has become fundamental in every application.
Prerequisiti	Knowledge of the topics treated in Computer Networks I is required.
Altre informazioni	See http://bartoli.inginf.units.it (teaching section)
Modalità di verifica dell'apprendimento	Written exam on exercises based on real applications, followed by an oral exam.
Programma esteso	TCP Implementation Technologies for Internet access based on private addressing (NAT/NAPT) TCP attacks. Attack models Authentication. Protocols APOP and NTLM. Attacks on password databases. Password salting. Kerberos: mutual authentication, secrecy, authentication delegation on a

local scale. Implementation.
Authentication and secrecy in PPP. PPP tunnel.
VPN: applications and SSL-based implementation
Single Sign On technologies for local deployment (LDAP, Kerberos) and geographic deployment
OAuth 2; OpenID Connect; SAML
Protected Wi-Fi: WPA personal and WPA enterprise.
Vulnerabilities and 0-day markets.
Web security: man-in-the-middle attacks to HTTPS;blic Key Pinning, Cross- Site Request Forgery, Cross-Site Scripting
Denial of service: attacks and defense.