Sicurezza dei Sistemi Informatici

Giovanni Bottazzi

CORSO DI LAUREA IN INGEGNERIA MEDICA
Università degli Studi di Roma – "Tor Vergata"
(Marzo– Giugno 2012)
gbottazzi73@gmail.com

Agenda…

- Introduzione
- Modelli di riferimento (ISO/OSI – TCP/IP)
- Encapsulation
- I livelli del TCP IP – protocolli, HW e indirizzamento
- Architetture LAN, MAN, WAN
- L'indirizzamento e il routing di Internet
- DNS, HTTP e WWW, EMAIL, FTP
- Proxy, Personal Firewall, Firewall, IDS, IPS
- La Governance in ambienti complessi
- Attacchi e contromisure

Agenda…

NR.	TITOLO	CONTENUTI	PERIODI STIMATI
1	*Introduzione, Fondamenti ISO/OSI, TCP/IP, Encapsulation.*	*Agenda del corso, principi alla base delle suite ISO/OSI e TCP/IP, paradigma di encapsulation.*	*3*
2	*Livelli TCP/IP - tecnologie, protocolli e formato pacchetti.*	*Principali tecnologie di riferimento, livello per livello, principali protocolli utilizzati e formato di pacchetto/frame. Digressione su indirizzamento IP v4, routing di Internet e cablaggio strutturato.*	*15*
3	*DNS, WWW, EMAIL, FTP.*	*Descrizione e principali funzionalità/protocolli.*	*3*
4	*Proxy, Personal FW, FW, IDS e IPS.*	*Descrizione e principali funzionalità.*	*3*
5	*Governance in ambienti complessi.*	*Architetture enterprise (INTRANET e DMZ), problematiche e approcci gestionali in ambienti complessi.*	*1*
6	*Attacchi e relative contromisure, alla pila TCP/IP ovvero a sistemi specifici.*	*Introdurre, possibilmente a tutti i livelli le principali tecniche di attacco (ARP/DNS POISONING, MITM, Injection e XSS, DOS, DDOS, SPAM) e relative contromisure (WEP/WPA, IPSEC, HTTPS/SSL/TLS, POP3S/SMTPS, STRONG AUTENHICATION, URL Filtering, ecc.) tralasciando tematiche afferenti il cracking degli algoritmi di cifratura. Esempio pratico di approccio ad un Audit di tipo "Double Blind" (discovery di sistemi e servizi).*	*5 (*)*

(*) dopo lezioni su algoritmi di cifratura

Introduzione

- Finalità. Concetti basilari di TCP/IP, cablaggio, principali sistemi e apparati di rete, sicurezza e management di realtà complesse.
- Approccio metodologico. Finché funziona tutto nessun problema.... Ma se ci sono problemi, il troubleshoting prima e la risoluzione dopo devono essere «approcciati» al giusto livello.
- Propedeuticità. I corsi che seguiranno, ed eventuali studi futuri professionali e personali, non prescinderanno dai concetti appresi in questa fase.....
- Stabilità. I progressi tecnologici cui assistiamo quotidianamente si basano su di un paradigma che «regge» dal 1978.....

Introduzione

Sicurezza. La sicurezza informatica è un concetto derivato e per questo motivo non assoluto.
L'ISO/OSI o TCP/IP non hanno al loro interno alcun concetto di sicurezza. Anzi le uniche finalità degli autori erano rivolte ad efficacia ed efficienza.
Molte delle problematiche di sicurezza derivano da funzionalità permesse per mere ragioni di efficienza ed amministrazione.
Probabilmente gli stessi autori non erano coscienti della rivoluzione in atto....

Introduzione

Sicurezza. L'informatica, o meglio la telematica, ha acquisito ormai un livello di «trasversalità» da rendere difficile l'individuazione di un ambito che direttamente o indirettamente ne sia estraneo. L'invasività è tale che i problemi di sicurezza informatica sono «degni» di un livello di attenzione almeno pari alle altre problematiche di sicurezza tecnologica.