FINALITÀ DEL SEMINARIO

Cosa dobbiamo sapere per difenderci come utenti web e come amministratori di server web.

Il web è diventato lo strumento principale di erogazione e di fruizione dei servizi in rete: dalla prenotazione di viaggi all'accesso al proprio conto corrente, dall'acquisto di beni materiali alla comunicazione elettronica. Proprio per questo motivo i servizi web sono oggetto di un numero crescente di attacchi, facilitati da tre fattori: debolezze intrinseche di alcuni protocolli, errata configurazione del server o del browser, comportamento ingenuo degli utenti.

Il seminario consentirà di apprendere le ultime novità e tecniche riguardo la sicurezza del web, imparando ad impostare correttamente i parametri di configurazione dei browser e dei server, nonché ad usare alcuni strumenti per difendersi da vari attacchi (es. man-in-the-middle, cross-site scripting, phishing, pharming, web bug, furto di credenziali di accesso).

Il seminario prevede spiegazioni teoriche intervallate con esempi pratici condotti su un sito web di test.

Programma dettagliato

- Brevi richiami sul funzionamento del web con pagine statiche o dinamiche (HTML, HTTP, CSS, JS, CGI, ASP, PHP).
- Attacchi passivi in rete per intercettare dati e password, inclusi strumenti di password cracking.
- Attacchi agli utenti finali del web (phishing, pharming e cross-site scripting); teoria, esemplificazioni pratiche e suggerimenti per mitigarne l'impatto.
- Il protocollo SSL (Secure Socket Layer), la sua configurazione sui browser e sui server e le sue debolezze, inclusi attacchi di tipo man-in-the-middle che saranno sperimentati tramite strumenti di attacco open-source.
- Uso dei certificati digitali nelle applicazioni web. Contromisure da prendere nel caso in cui un certificato sia stato associato in modo scorretto alle persone. Il caso Verisign-Microsoft e le sue conseguenze.
- Controllo accessi alle pagine web. L'autenticazione tramite username e password (basic/digest authentication), tramite certificato digitale (client authentication) e l'integrazione con l'autenticazione delle applicazioni e di dominio.
- Configurazione di sicurezza di un sito web gestito tramite Apache o IIS.

DESTINATARI

Il seminario si rivolge a chi si occupa di sviluppo, gestione ed organizzazione di sistemi informativi basati sul web e quindi in primo luogo a Sviluppatori di applicazioni/siti web e Responsabili della sicurezza e della qualità, ma risulta utile anche per Sistemisti, Responsabili della gestione di reti locali e geografiche e per chiunque sia interessato a conoscere la tecnologia e le applicazioni web.

ESPERTO

- **Diana Berbecaru**, Gruppo di Sicurezza Torsec, Dipartimento di Automatica e Informatica, Politecnico di Torino

  Laureata in Informatica e Dottore di Ricerca in Ingegneria Informatica e dei Sistemi, è Assegnista di Ricerca presso il Politecnico di Torino. Svolge la sua attività all'interno del gruppo di sicurezza Torsec del Dip. di Automatica e Informatica e si occupa di PKI, certificati digitali e sicurezza delle applicazioni Internet.
  Ha partecipato a vari progetti Europei nel campo della sicurezza dei sistemi informativi, quali AIDA, NASTEC e POSITIF.

PARTE SPERIMENTALE

Nell'ambito del seminario verranno svolte parti sperimentali mirate a verificare quanto descritto teoricamente.
La sperimentazione riguarderà i server Apache e IIS ed i browser IE, Mozilla e Firefox.

MATERIALE FORNITO

Verranno fornite copia del materiale didattico e CD coi programmi usati per dimostrare la fattibilità degli attacchi.

DATE

Chat: Giovedì 18 maggio 2006
Seminario: Giovedì 25 maggio 2006

SCADENZA ISCRIZIONI

Lunedì 15 maggio 2006

COSTO

Il costo del seminario è di 350.00 Euro + IVA.
La quota di iscrizione comprende la partecipazione al seminario, la consegna del materiale didattico, due coffee break e il pranzo, la possibilità di avere un contatto preliminare con il docente tramite chat e quella di contattare con modalità simili il docente in un momento successivo al seminario.