PinoLallo.com

Corso di Cybersecurity

Lezione 01: Fondamenti del Pentesting

Cos'è il Pentesting

Il pentesting è una valutazione controllata della sicurezza di sistemi e reti.

- Identifica vulnerabilità potenziali
- Simula attacchi reali
- Testa difese in condizioni realistiche

Tipi di Attacchi

Esistono vari tipi di attacchi nel pentesting:

- **Black Box** – nessuna conoscenza interna
- **White Box** – conoscenza completa
- **Gray Box** – conoscenza parziale

Nota: Ogni tipo ha i suoi vantaggi e svantaggi. Il Gray Box è spesso il più realistico.

Metodologie di Pentesting

Le metodologie seguono un approccio sistematico:

1. **Pianificazione** – definire scope e obiettivi
2. **Scansione** – identificazione vulnerabilità
3. **Exploitation** – sfruttamento controllato
4. **Reporting** – documentazione risultati

Strumenti Fondamentali

Ecco gli strumenti più utilizzati:

Strumento	Scopo	Categoria
Nmap	Scansione di rete	Recon
Metasploit	Framework di exploit	Exploitation
Burp Suite	Testing app web	Web
Wireshark	Analisi traffico rete	Sniffing
John the Ripper	Cracking password	Auth

Fasi del Processo

Il processo di pentesting include:

- **Pianificazione**: definire obiettivi e autorizzazioni
- **Scansione**: identificazione vulnerabilità (automated + manual)
- **Exploitation**: sfruttamento (etico!) per testare l'impatto
- **Reporting**: documentazione dettagliata per il cliente

Aspetti Etici

Il pentesting deve essere condotto in modo etico:

- Autorizzazione necessaria (contratto firmato)
- Rispetto delle leggi locali e internazionali
- Conseguenze legali per attività non autorizzate
- **Solo su sistemi di proprietà o con permesso esplicito**

Conclusione

Il pentesting è cruciale nella sicurezza informatica:

- **Competenze richieste** in crescita
- **Importanza** della formazione continua
- **Ethica** prima di tutto

Domande e Risposte

Spazio per domande degli studenti.

Nota: Incoraggiare la partecipazione attiva e discutere casi reali.