

TLS e Test Pratico di Pentesting

TLS e Test Pratico di Pentesting

TLS e Test Pratico di Pentesting

Lezione 05

- ID: tls-e-test-pratico
- Obiettivi: Comprendere il protocollo TLS e come testarne la sicurezza.

Introduzione al TLS

Il Transport Layer Security (TLS) è un protocollo crittografico utilizzato per garantire comunicazioni sicure.

Evoluzione da SSL a TLS

TLS rappresenta un miglioramento rispetto a SSL, introducendo nuove funzionalità di sicurezza.

Configurazione di un server TLS

Passaggi per installare un certificato TLS e attivare il supporto sul server web.

Test di Penetrazione

Come eseguire un test di penetrazione su un sistema protetto da TLS.

Strumenti per l'analisi della sicurezza TLS

Strumenti come OpenSSL e Qualys SSL Labs per valutare la sicurezza TLS.

Best Practices

Gestione delle chiavi e certificati per mantenere la sicurezza TLS.

Attacchi Comuni contro TLS

Discussione su attacchi noti e come mitigarli.

Conclusioni

Il TLS è essenziale nella sicurezza delle comunicazioni. Comprendere il suo funzionamento è cruciale.