AWS Cloud Pentesting

Presentazione del Corso

AWS Cloud Security

Amazon AWS sta assumendo una crescente importanza tra le aziende che utilizzano la tecnologia Cloud per ospitare e gestire i propri dati;

è quindi importante rilevare tempestivamente possibili configurazioni errate che possono essere sfruttate in un ambiente condiviso come il Cloud

Pentesting & Ethical Hacking

Il Pentesting è la pratica di scoprire e sfruttare possibili problemi di sicurezza nei sistemi IT

anche in ambiente Cloud è indispensabile condurre periodiche attività di pentesting, adottando metodiche adeguate al contesto condiviso

Pentesting in AWS Cloud

I pentester usano vari tool e tecniche di analisi dei sistemi per acquisire quante più informazioni possibili

data la particolarità dell'ambiente AWS Cloud, è necessario adottare un approccio e versioni specifiche dei tools utilizzati nei penetration test

Exploiting S3 Buckets

I bucket S3 sono una delle risorse principali che AWS utilizza per conservare i dati; i bucket S3 possono essere violati sfruttando configurazioni errate;

le configurazioni S3 errate possono quindi portare a perdite di dati e altri gravi problemi di sicurezza

Vulnerable AWS Services

Amazon AWS è scalabile e semplifica la configurazione di servizi basati su cloud, come i DB;

gli svantaggi di AWS sono analoghi a quelli dei comuni database, come possibili sql injection e sfruttamento di configurazioni errate

Pentesting Lambda Services

Lambda consente agli utenti di creare codice in grado di rispondere secondo necessità ai diversi eventi che si verificano all'interno dell'ambiente AWS;

le vulnerabilità in Lambda services possono portare allo sfruttamento dei servizi e alla scoperta di processi e oggetti riservati

Assessing AWS API Gateway

AWS API funge da gateway per le applicazioni che ospitano dati che potrebbero essere oggetto di accesso non autorizzato;

è quindi importante capire cos'è AWS API Gateway, come ispezionare le chiamate API e come correggere i problemi nelle chiamate API

Pentesting AWS with Metasploit

Metasploit è uno strumento di pentesting automatizzato, che consente di sfruttare facilmente le vulnerabilità note offrendo exploit preconfezionati

imparare a testare ambienti AWS utilizzando Metasploit è una skill indispensabile per ogni pentester

AWS Pentesting Best Practices

Il pentest è un'attività che va adattata sulla base del contesto specifico di sicurezza in cui viene eseguita;

le best practices sono essenziali quando si tratta di preservare l'integrità dei dati e delle applicazioni, prevenendo possibili responsabilità legali

Per saperne di più

Iscriviti al "Corso AWS Cloud Pentesting"