Descrizione generale

Informazioni generali del servizio

L'analisi viene svolta a fronte di un accordo commerciale/tecnico. Chi svolge questa attività è chiamato penetration tester o auditor e oggi anche con il più moderno nome ethical hacker, visto che si tenta di aggredire il sistema con le stesse logiche utilizzate da un hacker. Un gruppo di penetration tester è chiamato anche tiger team.I processi di penetration test possono essere effettuati in diverse modalità. La differenza consiste sulla quantità e qualità delle informazioni disponibili agli analisti riguardo i sistemi analizzati. I test Black Box non presuppongono precedente conoscenza dell'infrastruttura oggetto di analisi e gli esaminatori necessitano di determinare architettura e servizi dei sistemi prima di iniziare l'analisi.Nei test White Box sono invece fornite conoscenze dettagliate dell'infrastruttura da esaminare, spesso comprensive di schemi di rete, liste di indirizzi IP presenti nella rete. Esistono anche varianti a queste metodologie definibili Grey Box.I processi di analisi che vengono condotti in un penetration test hanno diversi tempi di azione in cui sono alternate fasi manuali e fasi automatiche. Vengono acquisite inizialmente le informazioni principali sull'architettura della piattaforma e sui servizi offerti. Dall'analisi di questi dati deriva la scelta di come condurre il passo successivo, consistente in una enumerazione dei principali errori e problemi. Software automatizzati uniti all'esperienza manuale dell'analista permettono quindi di evidenziare tutte le possibili vulnerabilità, incluse quelle più recenti e alcune ancora non di pubblico dominio. I problemi riscontrati sono quindi manualmente verificati e sono prese le evidenze, o prove, che certificano l'esistenza delle problematiche stesse.L'attività si conclude nello sviluppo della reportistica composta dal report di analisi sommaria dedicato al management o executive summary, contenente l'analisi dell'impatto di rischio di quanto riscontrato e tempistiche per l'azione di rientro o mitigazione delle problematiche riscontrate, e dal report tecnico, contenente l'analisi dettagliata dei problemi e la soluzione tecnica. Il penetration test va effettuato su sistemi esposti su Internet e comunque sulle piattaforme sensibili collegate a grosse reti, prima di entrare in esercizio, per avere una prova pratica della sicurezza di ciò che si espone.

ARWA di Alessandro Regolini
Via Lutteri, 3 - 38065 Mori, Trentino (TN) Italia
P.IVA IT 02148520220
C.F. RGLLSN82R12H612N
info@arwa.it