

Il Penetration Test è un'attività che prevede test di intrusione approfonditi a livello informatico e digitale.

Questo tipo di test si basa su tecniche di attacco reali finalizzate all'identificazione di vulnerabilità non note o comunque non rilevabili attraverso l'ausilio di soli strumenti automatici di scansione ed analisi al fine di dimostrare la reale penetrabilità del sistema dei livelli interessati.

I Penetration Test vengono svolti in gruppo da personale molto qualificato che prende il nome di Tiger Team.

Aree di Applicazione

Il servizio di Penetration Test può essere applicato in varie aree e contesti, dipendentemente dalle necessità di verifica della sicurezza richiesti. Tiger Security delinea la propria offerta per questo tipo di servizio in quattro macro aree.

•Network Penetration Test

Il Network Penetration Test va a prendere in esame una o più infrastrutture dal punto di vista della rete e dei servizi attivi su macchine presenti nella rete. Il focus di questa attività è quello dell'identificazione e dello sfruttamento di problematiche di sicurezza insite nella cattiva configurazione degli apparati e dei servizi e nella ricerca di bug applicativi o di protocollo all'interno dei servizi.

•Web Application Penetration Test

Il Web Application Penetration Test prende in esame una o più infrastrutture web sia dal punto di vista del servizio erogante il contenuto (WebServer, Database Server) che dal punto di vista della vera e propria applicazione che genera contenuto (Content Management System, CRM, Knowledge Base, Home Banking, ecc.). Il focus di questa attività è quello dell'identificazione e dello sfruttamento di problematiche di sicurezza insite nella

cattiva configurazione dei servizi e nel non corretto utilizzo di controlli sui dati in ingresso all'interno delle applicazioni web.

•Mobile Penetration Testing

Il Mobile Penetration Test è una attività che va a prendere in esame strumenti mobile come Tablet e Smartphone dal punto di vista prettamente applicativo e di sistema. Il focus di questa attività è quello dell'identificazione e dello sfruttamento di problematiche di sicurezza insite nella cattiva configurazione dei servizi e nella presenza di bug applicativi all'interno del sistema.

•Wireless Penetration Test

Il Wireless Penetration Test prende in esame strumenti di comunicazione senza fili che si occupano di erogare servizi di comunicazione internet, dati o voce. Il focus di questa attività è quello dell'identificazione e dello sfruttamento di problematiche di sicurezza insite nella cattiva configurazione degli apparati e dei protocolli e nella presenza di bug applicativi o di gestione che risiedono all'interno del sistema di erogazione del servizio.

Modalità di Applicazione

L'attività di Penetration Test è reputata molto utile anche per verificare i tempi di identificazione della minaccia e quindi di intervento del personale aziendale. Tiger Security eroga in accordo con il cliente questo tipo di attività in due modalità.

•Notified Penetration Test

Questa modalità di applicazione del Penetration Test è volta a curare nei minimi dettagli la delicatezza delle operazioni di test di penetrazione dei sistemi. Utilizzata per audit di sicurezza su infrastrutture critiche in produzione il Tiger Team (team che si occupa di individuare e verificare la penetrabilità del sistema) rimane in costante contatto per tutta la sua durata dell'attività con il Blue Team (team di difesa e monitoraggio).

•Hidden Penetration Test

Questa modalità di applicazione del Penetration Test è volta a verificare i tempi di identificazione della minaccia e quindi i tempi di risposta del Blue Team (team di difesa e monitoraggio). Con il solo accordo con la dirigenza l'attività di intrusione viene perpetrata all'insaputa di tutto il personale tecnico.

Modalità di Applicazione

Il Penetration Test può essere eseguito in diverse modalità, dipendentemente dallo scenario che il cliente desidera analizzare. Tiger Security offre questo tipo di attività in tre diverse modalità di esecuzione.

•Black Box

La modalità di esecuzione Black Box è volta a simulare un'attività di attacco da parte di un attaccante che non conosce alcun elemento di partenza della infrastruttura oggetto di verifica. L'obiettivo è quello di valutare quindi la resistenza e la non penetrabilità infrastrutturale da soggetti completamente esterni quali hacktivisti, governi ostili, competitor o comunque cyber criminali.

•Grey Box

La modalità di esecuzione Grey Box è volta a simulare un'attività di attacco da parte di un attaccante che in parte conosce elementi infrastrutturali interni alla piattaforma oggetto di verifica. L'obiettivo è quello di valutare la resistenza e la non penetrabilità di infrastruttura insider (non operanti in settori strategici) o competitor che possono aver acquistato informazioni circa le soluzioni tecnologiche utilizzare.

•White Box

La modalità di esecuzione White Box è volta a simulare un'attività di attacco da parte di un attaccante che conosce in modo estremamente dettagliato l'infrastruttura della piatta-

Tiger Security S.r.l.

Sede Legale: Via Bertina 8, Montefiascone (VT)

Sede Operativa: Via Velino 10, INT 1, Orvieto (TR)

P.IVA 02008450567

Fax : +39 0763 340498

Email : info@tigersecurity.it

forma oggetto di verifica. L'obiettivo è quello di valutare la resistenza e la non penetrabilità da insider (operanti in settori strategici) o da ex dipendenti.

Report di Attività

Al completamento di ogni attività vengono redatti dal Tiger Team due documenti ed un diario di bordo.

Il primo documento viene definito **Executive Summary** e contiene una relazione non tecnica dell'andamento dell'attività di Penetration Test con un summary finale riportante lo stato di penetrabilità dell'infrastruttura oggetto di verifica.

Il secondo, definito **Technical Summary** contiene una relazione tecnica con evidenze di compromissione (se presenti) che va a suggerire un piano di rientro operativo al dipartimento tecnico del cliente.