VA + PT

VULNERABILITY ASSESSMENT + PENETRATION TEST

Una errata configurazione degli apparati, configurazioni di default degli applicativi o un sistema non aggiornato potrebbero essere un punto di ingresso nell'infrastruttura. L'attività di VA+PT consiste nella messa in atto di scenari di attacco complessi e, oltre a quanto ispezionato con il VA, vengono verificate e messe alla prova anche vulnerabilità non pubbliche (potenzialmente presenti nel caso di software sviluppati ad hoc e/o non di larga diffusione). L'attività di PT è un'estensione del VA e, partendo dalle vulnerabilità emerse, verifica l'effettivo impatto cercando di penetrare all'interno del sistema obiettivo.

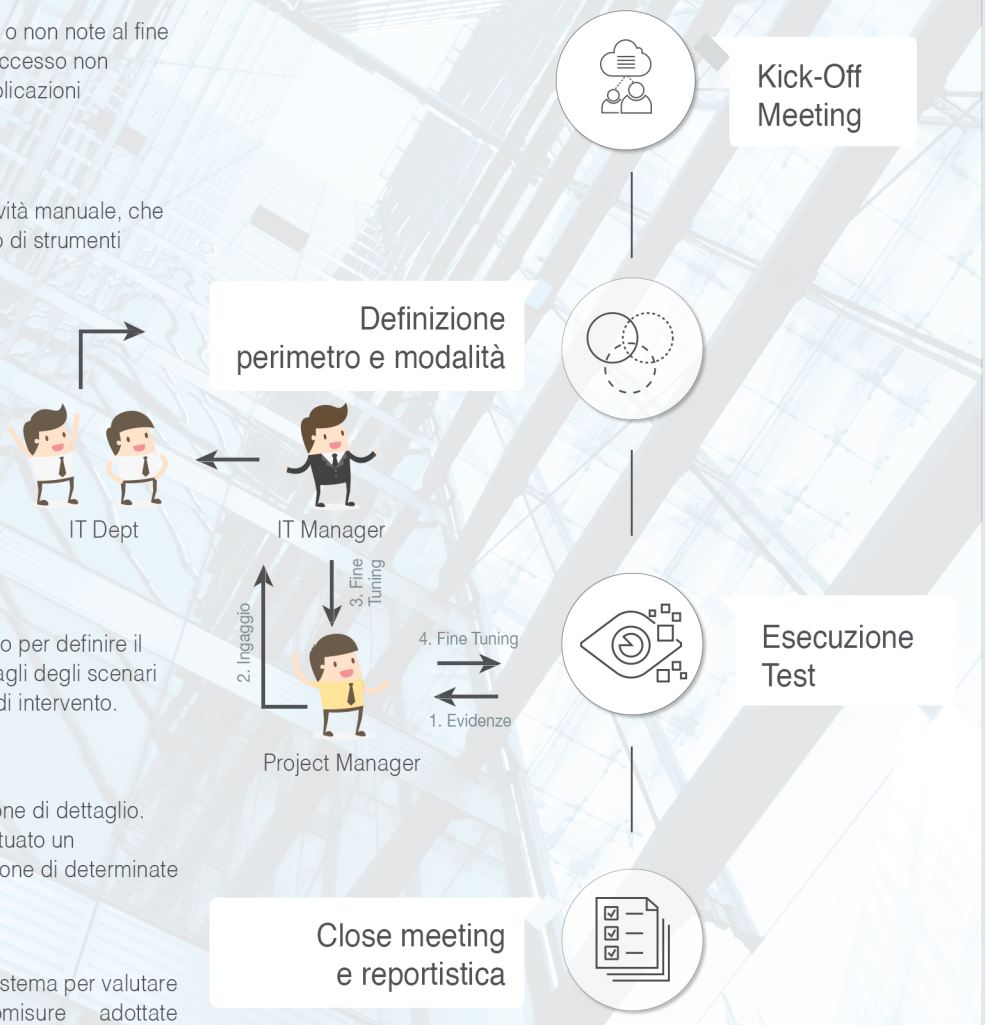
SCOPO
Utilizzare vulnerabilità note o non note al fine di testare la possibilità di accesso non autorizzato ai sistemi o applicazioni obiettivo.

COME
Il Penetration Test è un'attività manuale, che prevede tra gli altri l'utilizzo di strumenti automatizzati.

INPUT
Kick-Off Meeting, necessario per definire il perimetro da testare, il dettagli degli scenari di attacco, i modi e i tempi di intervento.

OUTPUT
Close-Off meeting e relazione di dettaglio.
A corredo può essere effettuato un affiancamento per la soluzione di determinate criticità.

FOLLOW UP
Si consiglia un'analisi del sistema per valutare l'efficacia delle contromisure adottate dall'azienda dopo 3/6 mesi dal primo PT.
È comunque sempre consigliato un PT a seguito di ogni cambiamento significato del sistema in esame.



Il potenziale impatto finanziario degli attacchi sulle aziende, dalle grandi alle piccole e medie imprese, è enorme. Oltre il 50% delle aziende analizzate nell'Annual Cybersecurity Report 2017 di Cisco ha dovuto affrontare severi controlli a seguito di una violazione.
I sistemi più colpiti sono quelli dei dipartimenti Operation & Finance, seguiti dalla perdita di reputazione del marchio e della fidelizzazione dei clienti. Per le aziende che hanno subito un attacco, l'effetto è stato notevole ed è preoccupante che i tempi medi impiegati per rilevare la minaccia si aggirino intorno ai 200 giorni.
- Il 22% delle aziende ha perso clienti - il 40% ha perso oltre il 20% della propria base di clienti.
- Il 29% ha perso fatturato - il 38% ha subito perdite per oltre il 20%delle entrate.
- Il 23% ha perso delle opportunità di business – il 42% ha preso oltre 20%.

Effettuare con regolarità attività di Ethical Hacking come Vulnerability Assessment e Penetration Test, abbatte i rischi di intrusione e perdita di dati sensibili dell'azienda. Non aspettare di avere subito un data breach!

NETMIND
SYSTEM INTEGRATOR