WPT

WIRELESS PENETRATION TEST

La rete wi-fi è ormai divenuta un elemento di elevata criticità in azienda e rappresenta un vettore di attacco preferenziale. Questo servizio permette di valutare il livello di sicurezza dell'accesso alla rete wireless, effettuando i test sia dall'esterno che dall'interno del perimetro aziendale. Nello specifico, vengono analizzate e sfruttate eventuali vulnerabilità legate all'algoritmo e alla chiave di accesso utilizzata, agli access point e alla loro configurazione.

SCOPO

Individuare vulnerabilità all'interno della infrastruttura wireless e sfruttarle al fine di simulare accessi non autorizzati alle applicazioni e ai dati in esse contenuti.

COME

Il WPT è un'attività manuale che prevede, tra gli altri, l'utilizzo di strumenti automatizzati. È prevista sia una attività on-site che un'attività da remoto.

INPUT

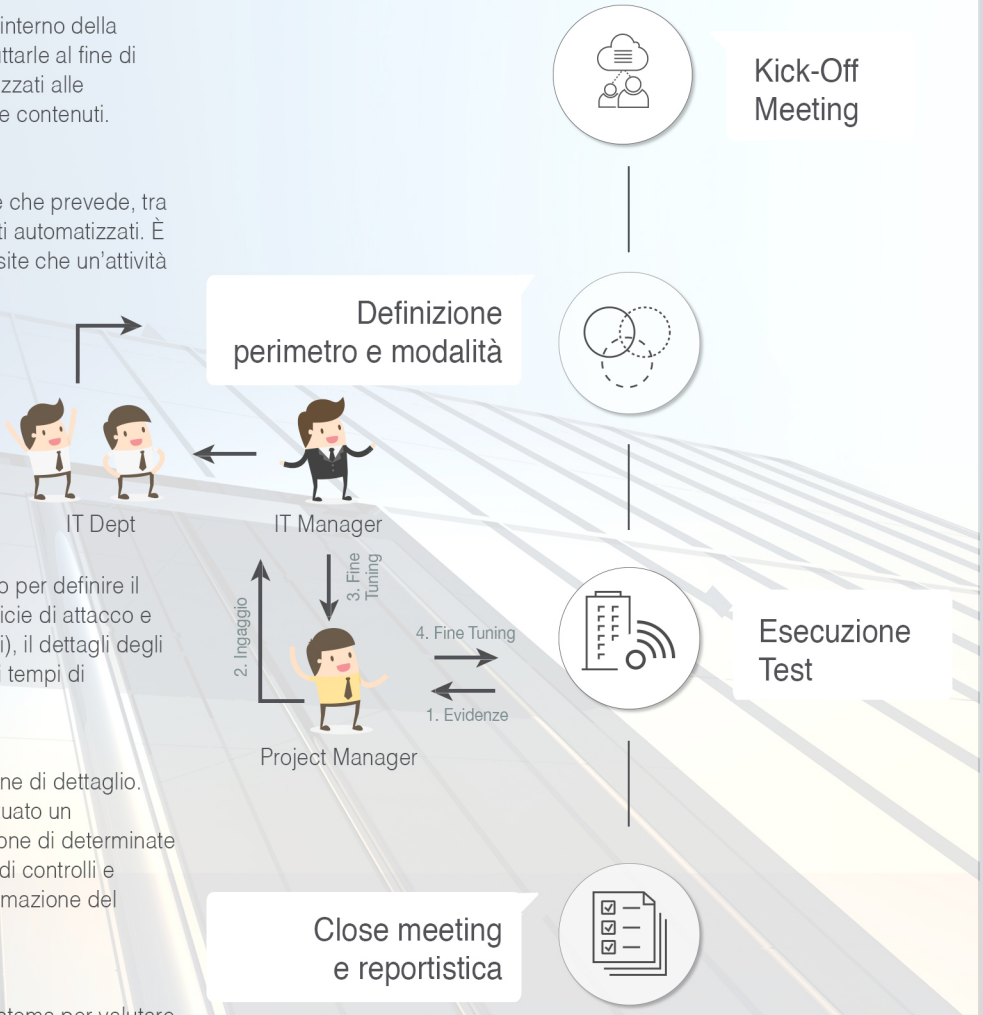
Kick-Off Meeting, necessario per definire il perimetro da testare (superficie di attacco e livelli di autorizzazione/utenti), il dettagli degli scenari di attacco, i modi e i tempi di intervento.

OUTPUT

Close-Off meeting e relazione di dettaglio. A corredo può essere effettuato un affiancamento per la soluzione di determinate criticità, l'implementazione di controlli e politiche di sicurezza, la formazione del personale.

FOLLOW UP

Si consiglia un'analisi del sistema per valutare l'efficacia delle contromisure adottate dall'azienda dopo 3/6 mesi dal primo WPT, e comunque a seguito di cambiamenti significativi dell'infrastruttura 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