# BLUE TEAM HACKING INFRASTRUCTURE VA/PT

Un bug di sistema, una configurazione errata, un documento sensibile divulgato inavvertitamente, o un utente con privilegi troppo elevati sono solo alcuni esempi di situazioni che possono esporre l'azienda a gravi conseguenze. I servizi di VULNERABILITY ASSESSMENT & PENETRATION TEST proposti da IMQ Intuity aggiungono, alla più tradizionale attività di analisi, anche azioni di *intelligence* quali la ricerca OSINT, l'analisi dei risultati contestualizzata alla realtà del cliente e la determinazione del reale valore di rischio per l'azienda.


## SERVIZI DI INFORMATION GATHERING

OSINT (Open Source INTelligence): attività di analisi effettuata nel dominio pubblico (Web, Dark Web, Deep Web) con l'obiettivo di cercare informazioni relative all'azienda, utili per la preparazione di un attacco o per la verifica di eventuali informazioni riservate diffuse in modo non autorizzato.

DIGITAL FOOTPRINTING: attività con la finalità di mappare in modo dettagliato ed esaustivo quanto un'azienda espone su Internet: indirizzi IP, servizi, domini e sotto domini.

## SERVIZI DI ASSESSMENT

NETWORK E WEB VULNERABILITY ASSESSMENT: attraverso una scansione strumentale ed un'analisi specialistica, il Vulnerability Assessment consente di identificare eventuali vulnerabilità presenti in un sistema o in un'applicazione ed assegnare un livello di criticità basato su standard internazionali.

NETWORK PENETRATION TEST: focalizzato a verificare l'impatto che eventuali vulnerabilità infrastrutturali potrebbero avere per un'azienda in caso di attacco informatico. Trattandosi di un'attività molto approfondita, un Penetration Test può far emergere vulnerabilità non rilevabili a livello strumentale durante un Vulnerability Assessment.

WEB APPLICATION PENETRATION TEST: volto a identificare e sfruttare eventuali vulnerabilità presenti nelle applicazioni web; in particolare, consente di evidenziare criticità nelle logiche applicative o in specifici controlli che sarebbero impossibili da evidenziare tramite un'analisi strumentale.
Per le attività di Web Application Penetration Test IMQ Intuity segue la metodologia indicata da OWASP: organismo di riferimento internazionale per i temi legati alla sicurezza delle applicazioni web.

**Operative Headquarters** Via Brunello Rutoli, 6 35129 Padova | Via Nazionale, 230 CAP 00184 Roma
**Registered Office** via M. F. Quintiliano, 45 - 20138 Milano
+39 0498170850
info@intuity.it

WI-FI PENETRATION TEST: L'attività consiste nello sfruttare le vulnerabilità delle reti Wi-Fi, sia aperte al pubblico che nascoste.

MOBILE APP PENETRATION TEST: l'attività consiste nel verificare la sicurezza di Mobile App sviluppate per gli ambienti Android e iOS, sia per gli aspetti legati al software installato sul dispositivo mobile che per quelli legati ai sistemi con cui la Mobile App comunica.

## LE FASI DEL SERVIZIO

### KICK-OFF
Ogni servizio inizia con un incontro con il cliente per definire le figure coinvolte nel progetto, le interazioni tra le diverse figure, le modalità operative di svolgimento del test e la discussione del perimetro delle attività.

### INFORMATION GATHERING – OSINT
L'attività prevede la raccolta di informazioni reperibili pubblicamente che possano risultare utili nella preparazione dell'attacco.

### VULNERABILITY ASSESSMENT
I sistemi e le applicazioni oggetto del servizio sono sottoposti ad analisi al fine di rilevare le vulnerabilità più evidenti.

### ANALYSIS
Le vulnerabilità riscontrate durante le fasi precedenti vengono raccolte, catalogate ed analizzate al fine di pianificare l'attività di Exploitation.

### EXPLOITATION – PENETRATION TEST
In questa fase viene verificato se le vulnerabilità riscontrate siano realmente sfruttabili e qual è il loro potenziale impatto sul business.

### REPORTING
Al termine delle attività di Exploitation, viene elaborata e fornita la documentazione, tecnica ed executive, contenente le informazioni rilevanti ottenute durante le varie fasi del processo.

### PRESENTATION
I report vengono presentati e discussi presso il cliente con l'obiettivo di chiarire i punti più significativi e definire un piano correttivo.

### REMEDIATION CHECK
IMQ Intuity include in tutte le attività di Assessment la possibilità di richiedere un rapido controllo da remoto sull'appropriata applicazione delle azioni correttive.

I servizi di Assessment (Vulnerability Assessment e Penetration Test) vengono erogati secondo una o più di queste metodologie:

- Blackbox: analisi del target senza possedere alcun tipo di autorizzazione d'accesso o informazione supplementare.
- Greybox: analisi del target avendo a disposizione alcune informazioni condivise.
- Whitebox: tutte le informazioni utili sono condivise, ove necessario anche i codici sorgente delle applicazioni da testare.