SCENARIO BASED RED TEAM

OFFENSIVE SECURITY

IMQ Intuity propone due diverse tipologie di esercizi di Red Teaming: **Business Focused** e **Scenario Based**. In entrambi i casi l'obiettivo è di creare una forte consapevolezza sul livello di rischio a cui è sottoposta un'azienda, simulando delle situazioni quanto più possibile vicine alla realtà, utilizzando mentalità e tecniche dei veri attaccanti.

BUSINESS FOCUSED RED TEAM:

La più realistica e completa simulazione di attacchi informatici alle aziende

Il primo servizio, definito **Business Focused Red Team**, è un esercizio durante il quale viene simulato un attacco informatico reale con uno sviluppo temporale di due mesi o superiore, fortemente caratterizzato da un approccio completamente *BlackBox*.

L'esercizio si propone di dimostrare se sia possibile creare un danno di business all'azienda, mettendosi esattamente nella condizione in cui si trova un attaccante esterno. Un vero attaccante, infatti, profila la propria vittima, ne cerca le vulnerabilità più critiche, sia tecnologiche che umane, e le usa per raggiungere il proprio scopo. Allo stesso modo si comportano gli specialisti IMQ Intuity. Nel caso di un *Business Focused Red Team* il "perimetro" è costituito dall'azienda stessa nella sua "totalità" e la ricerca del vettore di attacco è parte integrante del servizio stesso.

SCENARIO BASED RED TEAM:

Per **Scenario Based Red Team** invece, si intende una simulazione di attacco limitata ad uno o più scenari predefiniti. Questo tipo di esercizio ha come obiettivo principale quello di testare approfonditamente uno specifico contesto, indicato dal cliente o proposto da IMQ Intuity. In questi contesti l'attaccante si muove liberamente. Il test di uno scenario ha una durata variabile a seconda della sua complessità, del suo obiettivo o del tempo che si vuole dedicare alla simulazione.

Sede Operativa: Via Brunello Rutoli, 6 35129 | Padova
Sede Operativa: Via Nazionale, 230 CAP 00184 | Roma
Sede Legale: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it

DEFINIZIONE DI SCENARIO OPERATIVO

Contesto: situazione ipotetica da simulare.

Obiettivi da raggiungere: cosa si vuole verificare, quali sono le condizioni per cui la simulazione si considera terminata con successo.

Starting Point: dove si trova l'attaccante e in quale condizione opera.

Test Previsti: tipologia di test previsti; per alcuni scenari generici è difficile prevedere esaustivamente i test che potranno essere effettuati.

SCENARIO BASED PURPLE TEAM

Scenario Based Purple Team è un'analisi approfondita delle tecniche di attacco effettuate durante gli scenari, nel quale ha luogo un confronto fra Red Team e Blue Team. La condivisione delle informazioni fra i due team, permette uno scambio di prospettive che promuove il miglioramento continuo.

Sede Operativa: Via Brunello Rutoli, 6 35129 | Padova
Sede Operativa: Via Nazionale, 230 CAP 00184 | Roma
Sede Legale: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it

ESEMPI DI SCENARIO

SCENARIO "A"

Contesto: Il PC di un dipendente viene compromesso, l'attaccante è riuscito ad accedere e a prendere possesso del PC stesso, di fatto si trova nella rete aziendale con privilegi utente.

Obiettivi da raggiungere: accesso al file server, compromissione di un account di dominio.

Test Previsti: quanto è possibile fare avendo un accesso remoto ad un dispositivo, come ad esempio *priviledge escalation*, blocco dell'anti-malware locale, scansione della rete, *vlan hopping*, *lateral movement*, *reverse shell*, installazione di software, *password cracking*.

SCENARIO "B"

Contesto: Un consulente/ospite/esterno malintenzionato si trova all'interno dell'organizzazione. L'attaccante dispone di un suo PC con il quale cercherà di effettuare delle attività malevole.

Obiettivi da raggiungere: accesso a documenti riservati.

Starting point: il personale IMQ Intuity avrà accesso ai locali aziendali con una connessione alla rete prevista per gli utenti esterni.

Test Previsti: attività di *ethical hacking*, *lateral movement*, *WiFi cracking*, attività di *Socail Engineering* e ricerca documenti fisici, accesso a PC non custoditi, connessione a punti rete non autorizzati, *vlan hopping*.

ESEMPI DI SCENARIO

SCENARIO "C"

Contesto: Un hacker vuole creare un blocco al servizio di distribuzione di energia elettrica e gas naturale.

Obiettivi da raggiungere: accedere alla rete di controllo dei sistemi di distribuzione, accedere a sistemi rilevanti per l'erogazione dei servizi critici.

Starting point: il personale IMQ Intuity è connesso ad una rete interna con un proprio dispositivo. Non sarà in possesso di ha alcuna informazione tecnica e infrastrutturale relativa ai servizi di distribuzione: scopo del team IMQ Intuity sarà di identificare tali informazioni all'interno della rete e sviluppare una strategia utile per raggiungere gli obiettivi definiti.

Test Previsti: enumerazione dei sistemi produttivi, ricerca credenziali di default, attività di ricerca OSINT, passive fingerprinting dei sistemi di produzione, lateral movement, attività di Social Engineering.

SCENARIO "D"

Contesto: Azienda GDO. I negozi rappresentano un punto di criticità se non adeguatamente gestiti. L'azienda vuole conoscere il livello di rischio rappresentato da un punto vendita che viene attaccato.

Obiettivi da raggiungere: accedere ai sistemi di cassa, arrivare ai sistemi centrali sfruttando la connessione tra il punto vendita e la sede principale.

Starting point: il personale IMQ Intuity agisce come un malintenzionato, si reca presso il punto vendita con la propria dotazione e cerca di sfruttare gli entry point disponibili. L'attività inizia nella modalità Black Box e può proseguire in una modalità differente.

Test previsti: collegamento a punti rete disponibili, cracking del sistema WiFi, attività di Social Engineering, hacking dei sistemi raggiungibili tramite la connettività ottenuta, hacking di altri dispositivi fisici presenti nel punto vendita (sistemi di pagamento elettronico, sistemi di controllo accessi, etc), badge cloning.