Servizio di Penetration Test

Introduzione

AptGetDefence offre un servizio di Penetration Test avanzato, progettato per testare la sicurezza dei sistemi aziendali simulando attacchi informatici reali. L'obiettivo è identificare le vulnerabilità sfruttabili da potenziali attaccanti, garantendo la protezione dei dati e l'affidabilità delle infrastrutture aziendali. Il nostro Team di esperti fornisce un'analisi approfondita, soluzioni mirate per mitigare i rischi e un miglioramento continuo della sicurezza.

Obiettivi del Servizio

Il Penetration Test ha lo scopo di:

- Simulare attacchi informatici per identificare vulnerabilità e punti deboli.
- Testare la sicurezza dei sistemi e valutare la loro resistenza a potenziali exploit.
- Verificare l'impatto e la possibile estensione di una compromissione interna.
- Fornire un report dettagliato con soluzioni pratiche per mitigare le vulnerabilità.

Benefici del Servizio

- **Sicurezza proattiva**: Identificazione di vulnerabilità prima che possano essere sfruttate da attaccanti reali.
- **Valutazione della resilienza**: Simulazione di attacchi realistici per verificare la capacità di difesa del sistema.
- **Conformità normativa**: Garanzia di conformità con gli standard di sicurezza (GDPR, ISO27001, NIST, NIS2).
- **Protezione dei dati**: Riduzione del rischio di data breach e protezione delle informazioni aziendali sensibili.
- **Miglioramento continuo**: Identificazione di aree di miglioramento per una sicurezza costante e aggiornata.

Modalità di Test

Il nostro Penetration Test può essere eseguito in due modalità principali, a seconda delle necessità del cliente:

- **White-box**: In modalità white-box, il nostro Team ha accesso completo o parziale alle informazioni interne del sistema, come codice sorgente, configurazioni e credenziali di accesso. Questo approccio consente di testare l'intera

infrastruttura, simulando un attacco sia dall'interno che dall'esterno. Impersoniamo vari ruoli utente, eseguendo test approfonditi per analizzare ogni livello di accesso e valutare la sicurezza del sistema e delle sue componenti interne.

- **Black-box**: In modalità black-box, il nostro Team agisce come un attaccante esterno, senza alcuna conoscenza preliminare del sistema o delle sue configurazioni. Simuliamo un attacco come un hacker che cerca di compromettere il sistema partendo solo da informazioni pubblicamente disponibili, come un utente esterno che non ha accesso ai dati riservati.

Il Penetration Test può essere effettuato anche in due modalità geografiche/distintive:

- **Attacco Esterno (dall'esterno verso l'interno)**: In questa modalità, simula un attacco da parte di un hacker esterno che non ha accesso alla rete aziendale. Questo tipo di test mira a identificare vulnerabilità esposte su internet, come quelli dei server web, delle applicazioni online, delle configurazioni di rete e delle porte aperte.

- **Attacco Interno (dall'interno verso l'interno)**: Qui, simula un attacco da parte di un malintenzionato che ha già accesso alla rete aziendale, ma non ha privilegi di amministrazione. Questo scenario è utile per testare come un attaccante che ha superato le difese di perimetro possa muoversi lateralmente nella rete, ottenere privilegi elevati e compromettere sistemi sensibili, con l'obiettivo di simulare minacce interne come attacchi da parte di dipendenti o hacker che abbiano acquisito credenziali.

Personale Coinvolto

- **Azienda Cliente**:
  - **Responsabile IT/Rivenditore IT**: supervisione del processo.
  - **Team di Sicurezza IT**: verifica delle criticità riscontrate.
  - **DPO**: assicurarsi della conformità alle normative sulla protezione dei dati.
- **AptGetDefence**:
  - **Security Analyst**: esecuzione del Penetration Test.
  - **Security Consultant**: analisi dei risultati e suggerimenti di mitigazione.
  - **Project Manager**: coordinamento e gestione delle attività.

Output dell'Attività

- **Report di Penetration Test**: Documento dettagliato con elenco delle vulnerabilità identificate, livello di rischio e priorità di intervento.

- **Raccomandazioni di Mitigazione**: Suggerimenti pratici per risolvere le vulnerabilità e rafforzare la sicurezza.
- **Sessione di Debriefing**: Incontro finale per presentare i risultati e definire le azioni correttive.

Servizi Aggiuntivi Post-Penetration Test

AptGetDefence offre anche altri servizi complementari come il *Vulnerability Assessment*, che consente di eseguire una scansione più approfondita e continuativa delle vulnerabilità. Inoltre, offriamo il *Security Audit* per valutare la conformità alle normative di sicurezza e garantire che i sistemi siano sempre aggiornati e protetti contro le minacce.

Per ulteriori informazioni o per richiedere un preventivo, contattate AptGetDefence all'indirizzo ai seguenti riferimenti: www.aptgetdefence.com; customer@aptgetdefence.com