PENETRATION TEST

Il processo di Penetration Test è la metodologia di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato. L'analisi comprende più fasi ed ha come obiettivo evidenziare le debolezze della piattaforma fornendo il maggior numero di informazioni sulle vulnerabilità che ne hanno permesso l'accesso non autorizzato. L'analisi è condotta dal punto di vista di un potenziale attaccante e consiste nello sfruttamento delle vulnerabilità rilevate al fine di ottenere più informazioni possibili per accedere indebitamente al sistema. Tutti i problemi di sicurezza rilevati vengono quindi presentati al cliente assieme ad una valutazione del loro impatto nel sistema e nello scenario del business aziendale, fornendo inoltre una soluzione tecnica o proposta di migrazione e mitigazione del sistema.

I processi di Penetration Test possono essere effettuati in diverse modalità. La differenza consiste sulla quantità e qualità delle informazioni disponibili agli analisti riguardo i sistemi analizzati. I test "Black Box" non presuppongono precedente conoscenza dell'infrastruttura oggetto di analisi e gli esaminatori necessitano di determinare architettura e servizi dei sistemi prima di iniziare l'analisi. Nei test "White Box" sono invece fornite conoscenze dettagliate dell'infrastruttura da esaminare, spesso comprensive di schemi di rete, codice sorgente delle applicazioni e liste di indirizzi IP presenti nella rete. Esistono anche varianti a queste metodologie definibili "Grey Box".

I processi di analisi che vengono condotti n un Penetration Test hanno diversi tempi di azione in cui sono alternate fasi manuali e fasi automatiche. Vengono acquisite inizialmente le informazioni principali sull'architettura della piattaforma e sui servizi offerti. Dall'analisi di questi dati deriva la scelta di come condurre il passo successivo, consistente in una enumerazione dei principali errori e problemi. Software automatizzati uniti all'esperienza manuale dell'analista permettono quindi di evidenziare tutte le possibili vulnerabilità, incluse quelle più recenti e alcune ancora non di pubblico dominio.

I problemi riscontrati sono quindi manualmente verificati e sono prese le evidenze, o prove, che certificano l'esistenza delle problematiche stesse.

L'attività si conclude nello sviluppo della reportistica composta dal report di analisi sommaria dedicato al management o Executive Summary, contenente l'analisi dell'impatto di rischio di quanto riscontrato e tempistiche per l'azione di rientro o mitigazione delle problematiche riscontrate, e dal Report tecnico, contenente l'analisi dettagliata dei problemi e la soluzione tecnica. Il Penetration Test va effettuato su sistemi esposti su Internet e comunque sulle piattaforme sensibili collegate a grosse reti, prima di entrare in esercizio, per avere una prova pratica della sicurezza di ciò che si espone..

INFORMATIVA ASSESSMENT:

Il documento rilasciato certifica l'avvenuta verifica della sicurezza e solidità delle suddette strutture e procedure, allo scopo di prevenire al massimo livello il verificarsi di disservizi, intrusioni e violazioni della privacy.

Il Report è da considerarsi un documento di Vulnerability Assessment, andrà pertanto inserito nel Risk Assessment, da allegare al bilancio di fine anno dell'azienda.

LA SICUREZZA DELLE INFORMAZIONI

Definiamo lo scopo di questo documento come la ricerca di vulnerabilità che possano intaccare quattro aspetti chiave:

- **Disponibilità**: l'*accessibilità* motivata alle informazioni;
- **Integrità**: la *completezza* e la leggibilità delle informazioni;
- **Autenticità**: la *validità* delle informazioni;
- **Riservatezza**: la *possibilità* che solo chi è autorizzato possa leggere le informazioni.

La sicurezza richiede, quindi, che le informazioni e l'accesso alle stesse siano rigorosamente controllate

METODOLOGIA	PENTESTING
Info gathering 	*La prima parte, una delle più importanti, consiste nel collezionare informazioni riguardo I target da analizzare. E' fondamentale non tralasciare alcun dettaglio per ottenere con successo una reale rappresentazione di tutte le possibilità di attacco.* *STEPS:* *1.Network Discovery,* *2. Collecting Domain Names,* *3.Arch/Services identification*
Assessment 	*La seconda parte prevede procedure automatizzate lunghe ed elaborate che permettono di verificare un numero estremamente alto di vulnerabilità.* *STEPS:* *1.Network VA,* *2. Web Servers and Web Applications VA,* *3. Database VA*
Exploiting 	*La parte più significativa riguarda il controllo manuale delle potenziali vulnerabilità di ogni host ,delle sue porte e servizi, provando a superare ogni protezione della piattaforma stessa, avvantaggiandosi di eventuali errori di configurazione ed exploit o anche verificando possibili credenziali di default che garantiscano l'accesso al sistema.* *STEPS:* *1. Exploits sources,* *2. Automated Tools,* *3. Login Brute Forcing*