FABER SYSTEM

SCHEDA PRODOTTO

Innovation is our history

Vulnerability Assessment ICT e Penetration Testing

obiettivo

Il processo di Vulnerability Assessment ICT e Penetration Testing valuta l'efficacia dei sistemi di sicurezza attraverso la simulazione di attacchi che evidenzino eventuali rischi strutturali ed applicativi. L'obiettivo consiste nel prevenire future minacce basate sulle vulnerabilità riscontrate.

metodologia

La metodologia utilizzata si basa sulle indicazioni OWASP (Open Web Application Security Project, www.owasp.org) e OSSTMM (Open Source Security Testing Methodology Manual, www.osstmm.org) di cui alcuni Security Consultant sono attivi Contributor, nel rispetto degli standard di riferimento (ISO 17799, ISO 27001, Legge 196/2003).

Le attività comprendono:

1. **Interviste ai responsabili tecnici del progetto** allo scopo di individuare, a livello macro:
   - Architettura di rete
   - Perimetro dei servizi offerti
   - Gestione e accesso alle informazioni
2. **Scansioni automatiche** per individuare servizi che potrebbero essere utilizzati come punti di ingresso
3. **Esecuzione di un Penetration Test** atto a:
   - Identificare le eventuali debolezze nell'installazione e deployment dell'applicazione
   - Verifica dei sistemi e algoritmi di crittografia utilizzati
   - Verifica dei meccanismi di validazione dell'input
   - Verifica dei meccanismi di gestione delle sessioni
   - Verifica della possibilità di aggirare i meccanismi di autenticazione ed autorizzazione
   - Verificare della possibilità di escalation di privilegi
   - Verificare della possibilità di accedere o modificare i dati esposti dall'applicazione
   - Identificazione delle vulnerabilità che potrebbero portare ad accessi non autorizzati, utilizzo non appropria-to delle risorse, perdita dell'integrità dei dati
4. **Validazione manuale delle vulnerabilità identificate** nel caso l'identificazione sia avvenuta tramite strumenti auto-matici
5. **Classificazione delle vulnerabilità** sulla base della semplicità di exploit, effort necessario alla loro correzione e im-patto del possibile exploit sul business

La documentazione dei risultati contiene, per ogni vulnerabilità rilevata, un valore di difficoltà di exploiting, che considera il livello di accesso alla macchina, l'estensione della tecnologia richiesta e la conoscenza che l'aggressore deve avere per sfruttarla.

valore

Sulla base delle informazioni raccolte, viene attribuito un valore di **Business Impact**:

- **Basso**: per quanto prevedibile, l'attacco non ha risvolti economici o di danno, ma questo potrebbe variare in combi-nazione con altri attacchi
- **Moderato**: un impatto economico medio, o comunque quantificabile, possibile esposizione negativa in termini di pubbliche relazioni, furto o distruzione di dati rimediabili senza conse-guenze a lungo termine
- **Alto**: impatto economico alto, o non quantificabile, danni alla reputazione aziendale, distru-zione o sottrazione di informazioni con conseguenza non rimediabili

Faber System S.r.l.
Sede legale: Via Ettore Bugatti, 15 - 20142 Milano :: Tel. +39 02 8914031 Fax +39 02 817533 :: www.fabersystem.it
:: P. I./Codice Fiscale 07155170157 - Registro Imprese di Milano n. REA 1146459 :: Capitale Sociale € 100.000,00 I.V.