Italia

Scegli la certezza.
Aggiungi valore.

TÜV Italia srl - Ufficio di Roma - I-00196 ROMA p.zza Apollodoro 26

Spett.le RFI

Alla c.a. Ing. Argiolas

Oggetto: LINEE GUIDA MODALITA' DI ESECUZIONE DI PT DEL PREGETTO PIC

INTRODUZIONE

Scopo del documento

Le linee guida contenute in questo documento sono formalizzate in linea con quanto disposto dal progetto "Analisi di sicurezza della postazione PIC operativa".

Scopo del documento è descrivere quali macroattività sono richieste al fornitore del servizio di vulnerability assessment e penetration test sul sistema PIC nel periodo ottobre-gennaio 2009.

Le presenti linee guida sono da intendersi di natura organizzativa e sono applicabili, ciascuna per la propria area di competenza, ai controlli di vulnerability assessment e, ove applicabile, di penetration test, indipendentemente dalla tipologia di controllo applicata.

Destinatario

Sono considerati destinatari delle presenti linee guida: RFI SpA, TSF SpA, Hacking Team Srl.

Output finale

Output finale delle attività esercitate dal destinatario del documento è la redazione di un report di vulnerability assessment conformemente a quanto disposto da RFI nei documenti contrattuali Infrastruttura applicativa e di sicurezza – Evoluzioni 2008 per il Sistema applicativo PIC, ed in particolare all'abolizione della distinzione tra la cosiddetta VPN rossa e VPN verde per permettere l'accesso dei servizi intranet di Linea Diretta e del servizio di accesso web alla posta elettronica da parte delle postazioni operative.

Obiettivi complessivi del progetto

Verificare la congruità del valore di rischio residuo, dedotto nella fase di RA, con quanto determinato dalle prove di VA, nell'ambito delle attività di Evoluzione 2008 per il sistema PIC.

Riferimenti normativi, standard e metodologie

OWASP, OSSTMM, ISSAF, ISACA.

Presupposti operativi

Sono considerati i seguenti presupposti operativi:

Presupposto	Specifica
Indipendenza dall'utilizzo dei tool di analisi delle vulnerabilità adottati dai destinatari del documento	**Per quanto attiene lo scopo delle attività descritte oggetto delle presenti linee guida, si dichiara la totale indipendenza dai tool adottati per il vulnerability assessment, anche se l'utilizzo degli stessi (siano essi commerciali, open source o sviluppati ad hoc) deve essere documentato nel report conclusivo di attività (si rimanda al capitolo Reportistica per i dettagli)**
Indipendenza dalla metodologia utilizzata per l'analisi delle vulnerabilità adottati dai destinatari del documento	**Per quanto attiene lo scopo delle attività descritte oggetto delle presenti linee guida, si dichiara la totale indipendenza dalle metodologie organizzative ed operative cui ci si conforma per il vulnerability assessment, anche se l'utilizzo delle stesse deve essere documentato nel report conclusivo di attività (si rimanda al capitolo Reportistica per i dettagli)**
Indipendenza dall'utilizzo dei tool di penetration test adottati dai destinatari del documento	**Per quanto attiene lo scopo delle attività descritte oggetto delle presenti linee guida, si dichiara la totale indipendenza dai tool adottati per le funzioni di penetration test, anche se l'utilizzo degli stessi (siano essi commerciali, open source o sviluppati ad hoc) deve essere documentato nel report conclusivo di attività (si rimanda al capitolo Reportistica per i dettagli)**
Indipendenza dalla metodologia utilizzata per il penetration test adottati dai destinatari del documento	**Per quanto attiene lo scopo delle attività descritte oggetto delle presenti linee guida, si dichiara la totale indipendenza dalle metodologie organizzative ed operative cui ci si conforma per il penetration test, anche se l'utilizzo delle stesse deve essere documentato nel report conclusivo di attività (si rimanda al capitolo Reportistica per i dettagli)**
Esercizio delle attività di cui ai due punti precedenti di tipo gray box e/o white box	**Per quanto attiene lo scopo delle attività descritte oggetto delle presenti linee guida, si prevede che le attività stesse siano condotte con metodologie organizzative ed operative di tipo gray box e/o white box. Qualora, a seguito del modello di approccio all'assessment, uno o più dei controlli descritti nella presente linea guida non fosse applicabile, dovrà essere data apposita giustificazione nell'Executive Summary del report conclusivo (si rimanda al capitolo Reportistica per i dettagli)**
Indipendenza da altre policy applicabili	**Fanno eccezione le policy previste dalla certificazione ISO 27001:2005 di PIC/RIACE.**
Indipendenza da requisiti di security di tipo fisico o architetturale.	**Fanno eccezione le policy previste dalla certificazione ISO 27001:2005 di PIC/RIACE.**
Indipendenza dalla verifica delle logiche di business dei sistemi applicativi in uso	**La verifica della/e web application è spostata a valutazione successiva e indipendente dal presente progetto**
Indipendenza dalle metriche di backup/restore dei sistemi in uso e dalle verifiche di conformità all'uso dei file componenti le applicazioni (quali, ad esempio, valutazione di non adozione di versioni obsolete o palesemente errate o file non referenziati)	**La verifica della/e web application è spostata a valutazione successiva e indipendente dal presente progetto**
Non applicazione, per l'obiettivo della presente linea guida, di test di sessione su sistemi di tipo web application	**La verifica della/e web application è spostata a valutazione successiva e indipendente dal presente progetto**
Non applicazione, per l'obiettivo della presente linea guida, di test di	**La verifica della/e web application è spostata a valutazione successiva e**

validità di dati su sistemi di tipo web application	**indipendente dal presente progetto**
Non applicazione, per l'obiettivo della presente linea guida, di test di incubazione di validità su sistemi di tipo web application	**La verifica della/e web application è spostata a valutazione successiva e indipendente dal presente progetto**
Esecuzione del vulnerability assessment in ambiente di esercizio	
Esecuzione del vulnerability assessment su ambiente operativo ospitante web application	

LINEA GUIDA

Specifiche

Ciascuna linea guida è presentata sotto forma di scheda con la seguente struttura:

Titolo

Specifica il tipo di attività (o complesso di attività) cui la linea guida fa riferimento, per esecuzione di vulnerabilità assessment o penetration test.

Descrizione

Dettaglio della tipologia di attività di vulnerabilità assessment o penetration test cui si fa riferimento.

Processo

Indicazione delle funzioni tipiche di riferimento per il vulnerabilità assessment o penetration test cui la linea guida fa riferimento.

Output

Risultato minimo che TUV si attende dall'attività sottoposta a linea guida, da presentare singolarmente e raccolto in sintesi nella reportistica conclusiva, da stilare secondo quanto previsto al capitolo Reportistica, cui si rimanda.

Robustezza di policy

Descrizione

Le policy di restrizione del software di tipo user policy o group policy delineano l'elenco di applicativi eseguibili dall'operatore che alimentano una whitelist di riferimento. Il controllo di conformità della whitelist consente di verificare la corretta distribuzione delle policy, soprattutto in relazione ad eventuali sistemi di gestione host based che possono essere molto granulari

Processo

Verifica della solidità della whitelist con lancio applicazioni autorizzate e tentativo di lancio di set di applicazioni non autorizzate.

Verifica della policy applicata e dei fattori di restrizione dell'applicazione (hash, posizione in file system, origine, certificato)

Output

Dettaglio documentato della eseguibilità delle applicazioni di whitelist mediante checklist di controllo

Dettaglio documentato della non eseguibilità delle applicazioni fuori whitelist mediante checklist di controllo

Documentazione dell'uso delle policy, dei fattori di restrizione selezionati, dello strumento atto alla loro configurazione, con la schematizzazione minima seguente:

| restrizione (es. blocco di una determinata versione di software)

| controllo (es. controllo dell'hash)

| controllo applicato (si_no)

| metodo di applicazione del controllo(es. uso del tool XYZ)

Fingerprinting ed evidenza delle applicazioni

Descrizione

Conoscenza della versione e della tipologia dei sistemi IT al fine di individuare quali exploit sono eventualmente utilizzabili, quali vulnerabilità espongono l'asset a controllo remoto, eventuali problematiche di non corretta configurazione, adozione di schemi autorizzativi e di amministrazione dei sistemi suscettibili ad attacchi di tipo brute force o assimilabili, il tutto ai fini di una attività di analisi di vulnerabilità maggiormente specifica. L'obiettivo è giungere ad una conoscenza di tipologia e versione dei vari elementi software (con particolare riferimento agli application server lato web) che consentono di implementare i servizi di business.

Processo

Adozione di strumenti di analisi di http response header, acquisizione di risposte a richieste http volutamente non conformi o riferibili a servizi inesistenti, acquisizione di risposte a richieste basate su protocolli non noti al web server, utilizzo di tool che automatizzano test di tipo http fingerprint (sia offline che online), timeline delle variazioni dell'ambiente nel tempo (ad esempio, release precedenti di un portale web). Individuazione di applicativi residenti su sistemi che espongono un dato indirizzo IP allo scopo di elencare tutti i suddetti, compresa attività di VPN assessment. Sono comprese, allo scopo, anche le cosiddette tecniche di "google hacking" o analoghe metriche di acquisizione dati mediante l'adozione di funzioni (note o non documentate) dei motori di ricerca.

Output

E' considerato tipico output una elencazione di risorse raggiungibili e mappabili comprendenti:

| sistema operativo, build e livello di patch (se disponibile)

| application, build e livello di patch (se disponibile)

| netblock owner (se applicabile)

| IP (se applicabile)

| Ultima data di variazione (se applicabile)

| Timeline delle variazioni e release del sistema variato (se applicabile)

| Evidenza di application su una infrastruttura data, mediante individuazione di url non manifesti, porte non standard, disvelamento di virtual host

Verifica della configurazione dell'infrastruttura e hardening

Descrizione

La complessità intrinseca della parte infrastrutturale del sistema IT necessita di elementi di controllo a livello di configurazione dei sistemi di scambio informazioni a questo livello.

Questo controllo mira a valutare la vulnerabilità dell'infrastruttura, dei sistemi in back-end, dei sistemi di autenticazione, dello stato di aggiornamento della configurazione e patch level.

Processo

Analisi degli elementi infrastrutturali al fine di determinare come interagiscono e quali livelli di esposizione al rischio rappresentano.

Tutti gli elementi sono analizzati in assessment o mediante penetration test per determinare se posseggano o meno vulnerabilità note.

Tutti i tool di amministrazione dei sistemi vengono revisionati ai fini della possibilità di scalata dei diritti.

I sistemi di autenticazione sono valutati ai fini della resistenza ad elementi di accesso ed utilizzo dall'esterno o dall'interno in maniera impropria.

Sono altresì valutati gli schemi e le policy di patch management e di hardening di sistema.

Output

Sono considerati tipici output del sistema di verifica:

| controlli su VPN

| affidabilità contro malware in genere dei sistemi di back end e di autenticazione

| esiti di controlli su applicazioni cgi-based

| esiti di controlli su reverse proxy

| esiti di controlli su front-end server e application server

| esiti di controlli su database server o LDAP server

| analisi di robustezza di DMZ

| analisi robustezza ad accessi dall'interno dell''infrastruttura con collegamenti diretti all'infrastruttura stessa

| verifica patch level management e applicazione policy di hardening

Test sessioni SSL ed affini

Descrizione

I controlli afferenti a questa categoria mirano a valutare la robustezza dei sistemi di cifratura adottati, per valutare l'efficacia dei sistemi di cifratura stessa ad impedire accessi a sistemi di comunicazione altrimenti ritenuti sicuri. Rientrano in questa categoria controlli di tipo https e sull'uso dei certificati digitali.

Processo

Verifica della configurazione di SSL allo scopo di valutare l'impiego di cifrature non deboli.

Analisi del protocollo di cifratura.

Analisi dell'hash.

Analisi dei certificati digitali.

Inoculazione di certificati digitali errati e verifica degli esiti.

Output

Sono strutturati report di esito che tipicamente contengo i seguenti elementi:

| Risposte a richieste su porte https (standard o meno)

| Analisi della configurazione dei server web che erogano servizi di tipo https

| Analisi dei certificati digitali impiegati: validità dell'emissione da parte di AC (trusted o self-established), validità corrente del certificato, controllo di congruenza tra nome del sito e nome dello stesso riportato nel certificato (in questo caso, valutazione di virtual host o IP based virtual server)

| Esiti di inoculazione di certificati digitali errati

| Verifica di procedure di cifratura deboli.

Analisi dei log

Descrizione

L'analisi dei log mira a verificare se dagli stessi siano disponibili informazioni su errori o configurazioni utili per sfruttare vulnerabilità del sistema.

Processo

La verifica riguarda il riporto nei log di informazioni considerate sensibili (ai sensi della vigente normativa o in ogni caso classificate come tali, quali username/password), localizzazione di log e spazio assegnato, rotazione e refresh dei contenuti di log, uso dei log da parte degli amministratori ai fini di verifica di tentativi di attacco al sistema, backup dei log, validazione preventiva dei dati prima di inserirli nei log (attestazione di conformità).

Output

Tipici output dell'attività sono considerati i seguenti:

| contenuto dei file di log e sulla conformità alle normative cogenti in materia di memorizzazione (e trattamento) di dati sensibili e sulla validazione preventiva della conformità di contenuto rispetto alla scrittura dei dati sul log stesso.

| localizzazione dei log (stesso sistema che il log controlla o sistema diverso, vulnerabilità a log zapper sullo stesso server, centralizzazione di log su log server)

| spazi assegnati e sulla localizzazione degli stessi (suscettibilità a fill dello spazio ai fini di DoS)

| rotazione e refresh dei log (tempi di rotazione, spazi di rotazione, security policy applicabile, uso di compressione, permission garantite dal file system)

| backup dei log

| criteri di analisi dei log e parsing ai fini di determinare comportamenti anomali del sistema, focalizzati sull'individuazione di tentativi di accesso non conformi o comunque errori che necessitano analisi da parte dell'amministratore di sistema

Test di vulnerabilità sulle autenticazioni in genere

Descrizione

Rientrano in questa categoria le verifiche su dizionari di accesso di default o comunque considerati facilmente intellegibili, attacchi di tipo forza bruta, bypass degli schemi di autenticazione, memorizzazione delle password o password reset

Processo

Applicazione di categorie di accesso di default ai sistemi in uso (siano essi commerciali che open source), test di blank password o credenziali standard o “di fabbrica”.

Applicazione di attacchi all’autenticazione di tipo forza bruta, anche con strumenti progettati ad hoc.

Applicazione di metodologie di bypass dello schema di autenticazione

Utilizzo di metodi di verifica di memorizzazione di password o password reset

Output

Sono considerati tipici risultati i seguenti:

| applicazione delle credenziali standard o comunemente note del sistema in uso e verifica degli esiti

| applicazione di user/password facilmente intellegibili e comuni nell’ambito del sistema da verificare.

| esiti degli attacchi di tipo forza bruta, sia mediante tool che sistema progettato ad hoc (se applicabile), in conformità alla tipologia di autenticazione adottata (http basic o digest, html form)

| attacchi di tipo dizionario

| attacchi di tipo search (con o senza condizioni di applicabilità)

| esiti di bypass di autenticazione (richiesta di pagina diretta, modifica parametri di autenticazione, individuazione dell’id di sessione, sql injection su html form autentication)

| verifica sistema di password reset o reinvio di password per applicazioni basato su richiesta da email o basato su frase di sicurezza, verifica dell’accessibilità a password memorizzate localmente nel sistema client

Denial of Service, genericamente inteso

Descrizione

Scopo di queste verifiche è verificare la robustezza dei sistemi in ordine alle possibilità più utilizzate di provocare un Denial of Service dei sistemi stessi. Diversi processi descritte sono maggiormente significativi in condizione di assessment in gray box.

Processo

Analisi dei processi di lock di account

Analisi della suscettibilità ai buffer overflow

Analisi delle possibilità per gli utenti di scrivere dati su disco

Analisi del non rilascio di risorse

Analisi della possibilità di memorizzare eccessive risorse durante una sessione

Output

Sono considerati tipici output i seguenti:

| verifica della possibilità del sistema di memorizzare account utente e bloccarli ai fini di difesa da attacchi forza bruta congruente con robustezza del sistema stesso ai fini di non vulnerabilità ad attacchi DoS (adozione di coppie user/password non deboli)

| report di suscettibilità del sistema ad essere attaccato con codice che generi buffer overflow

| report sull'utilizzo dei log e sulla non possibilità per un utente di riempire lo spazio allocato per i flile di log generando blocchi di sistema

| report sulla suscettibilità del sistema a codice che impedisca il rilascio di risorse di sistema (risorse di memoria o file)

| report sul range di dati che può essere memorizzato dalla sessione utente

Verifica di robustezza a malware, genericamente inteso

Descrizione

Scopo di questa componente è controllare la robustezza del sistema a tentativi di infezione da malware (nella sua più ampia accezione) ed indipendentemente dal diver di tentata infezione.

Processo

Le attività di verifica, mediante penetration test, della robustezza dei sistemi al malware sono possibili in forma di static analysis o dynamic analysis indifferentemente, con opzioni contestualizzate alla tipologia di servizio di verifica.

Output

Sono considerati tipici output i seguenti:

| esiti di infezione da virus obsoleto

| esiti di infezione da virus recente

| esiti di infezione da virus recentissimo

| esiti di infezione da spyware, adware e simili

| esiti di infezione da macro virus

| esiti di infezione da file con attachment validi ma incubanti

REPORTISTICA

Il report di attività sarà composto da almeno tre sezioni obbligatorie. Ulteriori sezioni o sub sezioni potranno essere organizzate dai destinatari del presente documento qualora si ritenga necessario dettagliare le informazioni in modo da distinguerle per funzione (ad esempio per sistemisti, sviluppatori ecc.) o divisione (es. top management, middle management ecc.) di riferimento.

Le sezioni indispensabili sono:

Executive Summary

L'executive summary riepiloga l'esito complessivo degli elementi del vulnerability assessment e fornisce una sintesi dei risultati, confrontandoli con la sintesi del report precedentemente consegnato.

Si raccomanda di includere in questa sezione anche un dettaglio dell'inizio e fine dell'attività di assessment.

La sezione si chiude con l'indicazione delle implicazioni di quanto rilevato e delle azioni di genere che dovranno essere attuate, con indicazioni di tempi, risorse e responsabilità di massima secondo un modello di cronogramma.

Sinottico tecnico

In questa sezione sono delineati gli aspetti tecnici del risultato dell'assessment ed ha per destinatario il middle management di tipo tecnico.

In questa parte del report vanno delineati:

- obiettivi dell'assessment,
- target (in termini di elenco degli asset verificati, materiali ed immateriali)
- elenco dei test
- esito dei rischi rilevati e loro classificazione

Risultato dell'Assessment

In questa sezione sono descritti gli esiti di dettaglio dell'assessment, le vulnerabilità individuate, l'approccio necessario alla loro soluzione.

Questa è la sezione maggiormente tecnica ed è diretta al personale (i terno ed esterno) di riferimento diretto per le azioni da svolgere.

Ogni esito deve includere almeno i seguenti elementi:

- Codice identificativo dell'esito
- Descrizione dell'esito
- Screenshot che accompagna la descrizione (o altra evidenza, se applicabile)
- L'asset o elemento tecnico cui l'esito si riferisce
- Dettaglio tecnico della vulnerabilità riscontrata
- Soluzione ipotizzata (ipotizzabile)
- Livello di rischio e livello di impatto
- Strumento/metodologia adottato/a per il test della vulnerabilità

Uno schema di esemplificazione dell'esito delle attività di vulnerability assessment è il seguente:

Analisi/Tool	Asset	Esito	Note	Rischio

Ai fini dell'allineamento con quanto predisposto dal SiGSI occorrerà:

1. verificare la congruenza delle attività pianificate con le eventuali policies di sicurezza in atto
2. eseguire una valutazione preventiva dei rischi mutati (asset, vulnerabilità, minacce) derivanti dalle innovazioni apportate dal progetto

3. identificare le eventuali contromisure introdotte rispetto a quelle preesistenti (inserite nella dichiarazione di applicabilità) nel SiGSI
4. aggiornare il SiGSI (al termine del progetto) in modo che recepisca le eventuali differenze introdotte.

CONCLUSIONI

L'integrazione del progetto di RA/VA/PT con quanto prescritto nel presente documento (laddove applicabile e non già previsto) permetterebbe una più ampia riferibilità a standard e modelli atta a minimizzare le potenziali errori di valutazione.

L'algoritmo di valutazione del rischio residuo dovrà esser preliminarmente documentato così come i criteri di accettazione dei risultati ottenuti.