SPECIFICA DI ASSESSMENT PER I SERVIZI BPOL E BPIOL

Copia Archiviata Elettronicamente	File: SA_DBP_05_vulnerability assessment_SV_20051221

Copia cartacea Controllata in distribuzione ad enti esterni	N°:
Rilasciata al	
Copia cartacea non Controllata in distribuzione ad enti esterni	N°:

Versione	Pagina	Motivo della revisione	Data
1.0		Approvazione	21/12/05

Versione	Redazione	Verifica	Approvazione	Data
1.0	Roberto Ugolini		Dario Cassinelli	21/12/05

Indice

1 Scopo

Lo scopo del presente documento è quello di illustrare le attività richieste da Postecom per la realizzazione di un vulnerability assessment sistemistico/applicativo del servizio *BancoPostaonline* (BPOL) e del servizio *BancoPostaImpresa online* (BPIOL).

2 Applicabilità

I servizi internet oggetto della verifica sono:

- Bancopostaonline, raggiungibile a partire dall'indirizzo https://bancopostaonline.poste.it
- BancoPostaImpresa online, raggiungibile a partire dall'indirizzo https://bancopostaimpresaonline.poste.it/RBWeb/

L'analisi sarà svolta simulando attacchi verso i servizi concordati, al fine di verificarne la possibile compromissione della riservatezza, integrità e disponibilità delle informazioni e delle funzionalità gestite.

L'analisi sarà svolta in due fasi temporalmente distinte, ma da concludersi entro il primo trimestre del 2006:

- prima fase, per il servizio *BancoPostaonline*,
- seconda fase, per il servizio *BancoPostaImpresa online*.

Le modalità operative e la documentazione da produrre per ambedue le fasi sono descritte nei paragrafi successivi.

3 Modalità operative

Di seguito sono elencate le modalità operative che dovranno essere impiegate. Il Fornitore può proporre modalità alternative, esplicitandole espressamente.

ANALISI NON INVASIVA

1. IDENTIFICAZIONE E CLASSIFICAZIONE DELLE BANCHE DI DATI

   Questa fase ha lo scopo di identificare e di classificare le banche di dati gestite con il servizio oggetto della verifica. La classificazione è l'elemento chiave che permette di valutare il rischio effettivo di una vulnerabilità associata alla particolare banca di dati.

   La classificazione sarà effettuata in base ai parametri riservatezza, integrità, disponibilità e tenendo conto gli aspetti legati alla privacy.

2. ANALISI DELL'ARCHITETTURA

   Questa fase ha lo scopo di raccogliere il maggior numero di informazioni sull'obiettivo che si intende attaccare senza "toccare" l'obiettivo stesso. In particolare in questa fase è importante determinare, se pertinenti: *domini, blocchi di rete e gli indirizzi IP dei sistemi direttamente collegati ad internet*. Saranno effettuate interrogazioni ai seguenti servizi Internet (elenco non esclusivo):

   - Search engine
   - WHOIS database
   - WAIS database
   - DNS autoritativi primari e secondari (hidden)
   - WWW (mapping, hyperlink traversal)

   Inoltre saranno analizzati, tramite interviste conoscitive e la documentazione di supporto, l'architettura del servizio, i protocolli di comunicazione, i protocolli di sicurezza, i web server, i data server, gli application server ed i linguaggi di programmazione utilizzati. In questa fase sarà anche definita la "piattaforma" di attacco, anche in termini di dislocazione di rete.

ANALISI INVASIVA

3. SCANNING

L'obiettivo dello scanning è ottenere una verifica sulle informazioni ottenute nell'analisi dell'architettura, completandola con altre informazioni non ricavate precedentemente; ciò significa acquisire informazioni su quali IP dei blocchi di rete trovati nella fase precedente siano effettivamente contattabili, e, relativamente a tali IP, scoprire che servizi abbiano attivi e che sistemi operativi posseggano.

Le tecnologie impiegate sono (elenco non esclusivo):

- Network Ping sweeps
- ICMP queries
- Port scanning (TCP, UDP, RPC, stealth)
- Stack fingerprinting (remote OS detection)
- Application fingerprinting
- Firewalking (TTL modulation)
- TCP sequence number randomness
- Traceroute
- Transitive trust
- Network reverse mapping

4. ENUMERATION

Con questa fase si inizia "l'analisi invasiva" vera e propria, infatti si effettuano connessioni dirette ai server ed interrogazioni esplicite, il che potrebbe (a seconda della configurazione presente sui sistemi) originare dei log.

Attraverso l'enumerazione si vuole giungere a identificare, sulle macchine riscontrate come raggiungibili, degli account validi (list user accounts), delle risorse condivise (list file shares) e delle applicazioni attive sulle porte in ascolto (identify application).

Le tecniche utilizzate variano dai sistemi operativi delle macchine che vogliamo analizzare, di seguito una lista parziale:

- Finger
- Rusers
- X11
- SMB netbios shares
- SMB netbios resources
- NFS shares

- RPC mapping (portmap, common ports)
- Default accounts (SMTP, finger,..)
- SNMP
- Banner grabbing
- WWW (CGI, cookies, HTML sources,…)
- SSL (certificates, encryption used, numero di bits)

ATTACCO

5. GAINING ACCESS

Una volta ottenute le informazioni del punto precedente inizia il vero e proprio attacco che ha come obiettivo il riuscire a compromettere la riservatezza, l'integrità e la disponibilità nel sistema remoto, delle informazioni e delle funzionalità gestite.

I metodi utilizzati anche in questo caso dipendono dal sistema operativo della macchina, ma si basano sostanzialmente sulla ricerca di password corrispondenti agli utenti trovati (password guessing), sullo sfruttamento di errori progettuali delle applicazioni e servizi attivi sul server (buffer overflow, attacchi data driven, ecc.) o del sistema operativo stesso.

La lista di tecniche e tecnologie impiegate in questa fase varia moltissimo a seconda dello scenario rilevato nelle fasi precedenti, un elenco non esaustivo è riportato di seguito:

- Cross-site scripting
- Parameter tampering
- Hidden field manipulation
- Backdoors e opzioni di debug
- Stealth commanding
- Forceful browsing
- Buffer overflow
- Cookie poisoning
- Configurazioni errate
- Vulnerabilità note
- SQL injection
- Attacchi http
- Attacchi Man-in-the-Middle
- Attacchi Denial Of Service

4 Documentazione prodotta

Nella fase di assessment il Fornitore deve:

- rilevare le vulnerabilità e definire il fattore di rischio assoluto e quello reale (al fine di eliminare i falsi positivi ed in riferimento al contesto ambientale e topologico in cui il sistema si trova, e con riferimento alla banca di dati coinvolta);
- attribuire ad ogni vulnerabilità una valutazione del grado di SEVERITA' (Alta / Media / Bassa). La severità delle vulnerabilità prese in considerazione deve essere valutata ispirandosi alle classificazioni più diffuse in ambito internazionale (CVE, OSVDB, NESSUS ecc.);
- raggruppare, ove possibile, le varie vulnerabilità in classi omogenee: la tabella delle classi è fornita dal Responsabile dei Servizi Sicurezza di Postecom al Fornitore.

Il Fornitore produrrà un documento contenente l'elenco dei sistemi/applicazioni testati, la descrizione delle vulnerabilità riscontrate con indicazione del livello di rischio e le soluzioni correttive, anche architetturali, suggerite per elevare il livello di sicurezza.

La documentazione prodotta indicherà inoltre, relativamente alle azioni correttive, l'eventuale prodotto, classe di prodotto, intervento software che possa risolvere il problema evidenziato.

5 Impegni

E' necessario che il Fornitore si impegni esplicitamente al rispetto della riservatezza delle informazioni, al rispetto puntuale della Specifica di Assessment (ambito, tempistica e modalità operative) e alla restituzione di tutti gli elaborati e dei risultati intermedi.