]HackingTeam[

Milano, 23 Dicembre 2005

Spett. le
Postecom S.p.A.
Ufficio Acquisti
Via Cordusio, 4
20123 Milano

Offerta n. 20051223.mb55

Alla c. att.ne : Dr. Alessandro Verdiani

Oggetto: Offerta per attivita' di Vulnerability Assessment per i servizi internet BancoPostaOnline e BancoPostaImpresaOnline

A seguito della gradita richiesta, e in base alle specifiche descritte nel file SA_DPB_05_vulnerability assessment_SV_20051221, vi sottoponiamo la nostra proposta per il servizio in oggetto.

In attesa di un vostro gradito riscontro, vi porgiamo i nostri più cordiali saluti.

Hacking Team Srl

Marco Bettini
Key Account Manager

Offerta per servizio di Vulnerability Assessment per i Servizi Internet BancoPostaOnline e BancoPostaImpresaOnline

Titolo documento:	*Tipo documento:*	*Versione*:
Vulnerability Assessment Postecom 20051223.mb55	**Offerta**	1.0

SOMMARIO

1. RICHIESTA DEL CLIENTE

Postecom S.p.A. richiede di formulare una proposta, con relativa offerta economica, relativa a un intervento di Vulnerability Assessment sistemistico/applicativo che interessi i servizi internet di BancoPostaOnline (BPOL) e BancoPostaImpresaOnline (BPIOL) al fine di verificarne la possibile compromissione della riservatezza, integrità e disponibilità delle funzionalità e delle informazioni gestite.

I servizi internet oggetto della verifica sono:

- BPOL raggiungibile a partire dall'indirizzo https://bancopostaonline.poste.it
- BPIOL raggiungibile a partire dall'indirizzo https://bancopostaimpresaonline.poste.it/RBWeb/

Si specifica inoltre che i seguenti punti saranno compresi nei risultati della consulenza in oggetto:

- Documento tecnico che riporti le vulnerabilità individuate e i passi necessari per eliminarle

- Documento di presentazione per il management in forma di *slides*.

2. DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA

Un attacco compiuto da hacker reali segue di norma la traccia che segue. Le attività di Ethical Hacking da noi eseguite tentano di emulare al 100% il comportamento di un vero hacker. Il test, quindi, verrà condotto in modalità anonima ("black box").

Analisi non invasiva

1. IDENTIFICAZIONE E CLASSIFICAZIONE DELLE BANCHE 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 di riservatezza, integrità, disponibilità e tenendo conto degli aspetti legati alla privacy.

2. ANALISI DELL'ARCHITETTURA (FOOTPRINTING)

   Questa fase ha lo scopo di raccogliere il maggior numero di informazioni sull'obiettivo che si intende attaccare senza "toccare" l'obiettivo stesso, ovvero effettuando una cosiddetta "analisi non invasiva". In particolare in questa fase si cerca di determinare: *domini, blocchi di rete e indirizzi IP dei sistemi direttamente collegati ad internet*. Gli strumenti utilizzati sono: tecnologie di sniffing, traffic interception, DHCP discovery, IP discovery, interrogazione DNS, interrogazione WINS.

   Saranno effettuate interrogazioni ai seguenti servizi Internet:

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

Con interviste conoscitive e documentazione di supporto, saranno analizzati 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 mappa più dettagliata possibile del sistema da attaccare. Ciò significa acquisire informazioni su quali indirizzi IP dei blocchi di rete trovati nella fase precedente siano effettivamente "contattabili" (IP discovery), quali servizi siano "attivi" (TCP/UDP port scan) e, infine, quali sistemi operativi "posseggano". Gli strumenti generalmente utilizzati sono: interrogazioni ICMP (hping), scansione delle porte TCP e UDP (nmap, rascan), fingerprint dello stack (nmap, ettercap), application fingerprinting, firewalking, Traceroute, Network reverse mapping, Transitive trust.

4. ENUMERATION

Con questa fase si inizia l'"analisi invasiva". Si effettuano, infatti, connessioni dirette ai server e "interrogazioni" esplicite. Tali attività potrebbero, a seconda della configurazione presente sui sistemi target, originare dei logs sui sistemi (tipicamente su sistemi di controllo). Attraverso l'enumerazione si vuole giungere a identificare, sulle macchine riscontrate come raggiungibili, account validi (list user accounts), risorse condivise (list file shares) e applicazioni attive sulle porte in ascolto (identify application). Le tecniche utilizzate variano a seconda dei sistemi operativi delle macchine che si vogliono analizzare, ad esempio:

- 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 target, 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.

Analisi Applicativa

L'oggetto di questa parte di attività sarà il tentativo di accesso e di verifica della sicurezza dell'applicazione o del portale in oggetto.

L'attività comprende l'analisi dell'applicazione in termini architetturali, verranno analizzate le configurazioni delle macchine interessate, sia a livello di sistema operativo che applicativo.

L'attività di security audit dell'applicazione web identifica in modo completo le classi di attacco, in particolare saranno testate:

- 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

Opzionalmente è possibile ripetere le stesse attività in “user-mode” o “white box”. Ciò significa che, preventivamente, dovrà essere creato un account tramite le usuali procedure di attivazione al fine di permettere a Hacking Team di accedere come utente autorizzato e verificare se tale utente è in grado di accedere a informazioni alle quali non ha diritto.

Non saranno accettati account di altro tipo (di test interno, amministrativi, etc.) poiché non fornirebbero la corretta valutazione circa il rischio che un utente registrato possa cercare di accedere in modo fraudolento ad informazioni per cui non è autorizzato.

3. DOCUMENTAZIONE UTENTE

Nella fase di assessment verranno:

- rilevate le vulnerabilità e definito 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);
- attribuita 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.);
- raggruppate, ove possibile, le varie vulnerabilità in classi omogenee: la tabella delle classi sarà fornita dal Responsabile dei Servizi Sicurezza di Postecom

Verrà, inoltre, prodotto un documento contenente:

A. **Topologia rilevata**
B. **Dettagliata descrizione del metodo e degli strumenti**
C. **Elenco delle vulnerabilità riscontrate e relative contromisure**
D. **Elenco dei sistemi/apparati acceduti in modo non autorizzato**
E. **Descrizione della catena di eventi che hanno portato all'accesso della rete/sistema/applicazione**
F. **Eventuali esempi di dati/informazioni riservate ottenuti**

Sarà inoltre allegata una descrizione dei possibili miglioramenti che potrebbero essere applicati ai sistemi e ai servizi unita all'elenco, supra vendor, delle soluzioni tecnologiche e/o dei prodotti da adottare per incrementare il livello di security del sistema informativo.

.

4. DOCUMENTI NECESSARI

Per dare inizio alle attività sarà necessaria la sottoscrizione della liberatoria che autorizzi Hacking Team all'attività di attacco precedentemente descritta.

Inoltre, Hacking Team con il documento NDA allegato, si impegna 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.

5. RESPONSABILITÀ

Sarà responsabilità di Hacking Team completare il presente progetto secondo quanto specificato, fornendo al Cliente la documentazione citata.

Sarà responsabilità del Cliente garantire, ove necessario, l'accesso ai locali preposti, nonché la disponibilità di una persona durante le attività previste dal presente progetto.

La presenza di tale persona permetterà a Hacking Team di spiegare nel modo più rapido ed efficace le attività svolte, sia in termini di tecniche che di strumenti.

6. TEMPI DI REALIZZAZIONE

L'attività di cui sopra verrà svolta in due fasi distinte e, comunque, verrà completata entro il primo trimestre 2006.

7. OFFERTA ECONOMICA

Pos.	Descrizione	Costo a corpo
1	**Vulnerability Assessment servizi internet BPOL e BPIOL (black box)**	**€ 13.500,00 (tredicimilacinquecentoeuro)**

Le attività verranno svolte da:

- un senior security engineer il cui costo giornaliero è di € 750,00
- un security engineer il cui costo giornaliero è di € 650,00

Opzionalmente, proponiamo anche la ripetizione dell'attività in "white box" che, come precedentemente descritto, dietro il rilascio di credenziali utente consente di verificare a quali informazioni può accedere un utente accreditato, anche senza averne diritto.

Pos.	Descrizione	Costo a corpo
2 Opzionale	**Vulnerability Assessment servizi internet BPOL e BPIOL (white box)**	**€ 7.500,00 (tredicimilacinquecentoeuro)**

8. CONDIZIONI GENERALI

I prezzi indicati sono da considerarsi IVA esclusa.

Sono escluse le spese di trasferta eccetto che per la fase iniziale di raccolta informazioni e presentazione risultati finali.

Validità offerta: 30gg

Fatturazione: 50% all'ordine

30% alla consegna della documentazione finale relativa a BPOL

20% alla consegna della documentazione finale relativa a BPIOL

Pagamento: 30 gg data fattura