Milano, 5 Novembre 2004

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

Offerta n. 20041105.m02

Alla c. att.ne : Dr. Alessandro Verdiani

Oggetto: Offerta per attivita' di Vulnerability Assessment per il portale www.poste.it

A seguito della gradita richiesta, 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 il Portale www.poste.it

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 che interessi il portale www.poste.it al fine di verificarne la possibile compromissione della riservatezza, integrità e disponibilità dei sistemi coinvolti e delle informazioni gestite.

Il dimensionamento dell'attivita' richiesta e' il seguente:

- Network di Indirizzi IP : 62.241.0.0/20

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

2.1. Security Probe

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.

Analisi non invasiva

1. 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 alla rete interna*. Gli strumenti utilizzati sono: tecnologie di sniffing, traffic interception, DHCP discovery, IP discovery, interrogazione DNS, interrogazione WINS.

2. 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.

Analisi invasiva

3. 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

4. GAINING ACCESS

Una volta ottenute le informazioni del punto precedente, inizia il vero e proprio attacco che ha come obiettivo riuscire a “entrare” nel sistema remoto. 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.

5. ESCALATING PRIVILEGES

L’obiettivo di questa fase è sfruttare i risultati ottenuti nella fase precedente per ottenere il pieno controllo del sistema remoto attaccato. Ciò si ottiene, per esempio, reperendo i files presenti sul sistema che contengono le password (/etc/passwd, SAM, ecc.) e tentando di decifrare le password in essi contenute (password cracking), oppure utilizzando appositi exploits.

3. DOCUMENTAZIONE UTENTE

Oltre a ciò specificatamente richiesto nel capitolo 1 (RICHIESTA DEL CLIENTE), al termine dell'attività sarà fornito un report che conterrà:

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. PIANO DI INTERVENTO

4.1. Attività (tipologie)

Attività
Attività di Ethical Hacking dall'esterno
Incontro per la presentazione dei risultati e di tutto il materiale prodotto: • Report Direzionale. • Report tecnico dettagliato con indicazione delle possibili soluzioni.

Il materiale prodotto sarà fornito su supporto cartaceo e/o supporto digitale.

4.2. Documenti necessari

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

5. RESPONSABILITÀ

Sarà responsabilità di Hacking Team completare il presente progetto secondo quanto specificato nella definizione delle funzionalità iniziali, 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 conclusa entro 4 settimane dalla ricezione dell'ordine e, comunque, entro il 10 dicembre 2004.

7. OFFERTA ECONOMICA

7.1. Quotazione a corpo

Pos.	Descrizione	Costo a corpo
1	**Vulnerability Assessment portale www.poste.it**	**€ 26.000,00 (ventiseimilaeuro)**

La documentazione e la reportistica sono comprese nel costo dei servizi esposti.

7.2. Condizioni generali

I prezzi indicati sono da considerarsi IVA esclusa
Validità offerta: 30gg
Fatturazione: 50% all'ordine
50% alla consegna della documentazione finale
Pagamento: 30 gg data fattura
Coordinate Bancarie: Unicredit Banca
L.go Donegani - Milano
ABI 02008 CAB 01621 C/C 000010228244 CIN A