]HackingTeam[

Milano, 31 Agosto 2007

Spett. le
DI.GI. Security
Via Valtellina, 63
20159 Milano

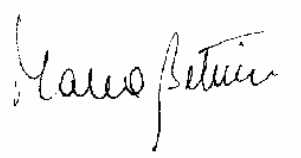
Offerta n. 20070831.mb32

Alla cortese attenzione: Dr. Davide Dell'Orto
Dr. Andrea Ghislandi

Oggetto: Offerta per attività di Vulnerability Assessment per il Cliente ATA Hotels

A seguito della Vostra 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 S.r.l.
Marco Bettini
Key account Manager



Offerta per attività di Vulnerability Assessment e Penetration Test per il Cliente ATA Hotels

SOMMARIO

1. STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	31 Agosto 2007	Emissione Offerta

2. RICHIESTA DEL CLIENTE

Vedi allegato tecnico

3. DETTAGLI TECNICI DEI SERVIZI PROPOSTA

3.1. Security Probe

Un attacco compiuto da hacker reali segue di norma la traccia riportata di seguito. 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 a Internet*. Gli strumenti utilizzati sono: Search Engine, Whois server, Arin database, interrogazione DNS, ecc.

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" dall'esterno (IP discovery), quali servizi siano "attivi" (TCP/UDP port scan) e, infine, quali sistemi operativi "posseggano". Gli strumenti utilizzati sono: interrogazioni ICMP (hping2, ecc.), scansione delle porte TCP e UDP (strobe, netcat, nmap, ecc.), fingerprint dello stack (nmap, ettercap).

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 vogliamo analizzare.

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 overflows, attacchi data driven, ecc.) o del sistema operativo stesso.

5. ESCALATING PRIVILEGES[1]

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

[1] Vogliamo specificare che, considerata la natura della presente offerta, le nostre attivita' *non si spingeranno in nessun caso oltre questo punto (ESCALATING PRIVILEGES) a meno di una specifica autorizzazione in tal senso da parte del cliente.* In altre parole, si cerchera' di **dimostrare l'effettiva possibilità di assumere il controllo dei sistemi senza apportare alcuna modifica agli stessi.**

password (/etc/passwd, SAM, ecc.) e tentando di decifrare le password in essi contenute (password cracking), oppure utilizzando appositi exploits.

Consolidamento

6. PILFERING

Se si giunge a questa fase significa che si è ottenuto il pieno controllo del sistema target. Quindi è bene valutare la configurazione del sistema stesso al fine di capire se, dove e cosa il sistema registra (logs). I sistemi di auditing saranno eventualmente disabilitati (es. con Win NT mediante auditpol). A questo punto la macchina in oggetto può diventare una "testa di ponte" per attaccare altre macchine. In tal caso saranno reperite informazioni riguardanti altri sistemi.

7. COVERING TRACES AND CREATING BACK DOORS

Prima di abbandonare il sistema "conquistato" vengono cancellati gli eventuali logs che hanno registrato la presenza clandestina ed eventualmente installati trojan o back-doors che consentano di rientrare facilmente sulla macchina in un secondo momento. Può essere utile anche installare tools nascosti quali sniffers o keyloggers al fine di catturare altre password del sistema locale o di altri sistemi ai quali utenti ignari si collegano dalla macchina controllata.

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

4. DOCUMENTAZIONE UTENTE

Oltre a ciò specificatamente richiesto nel capitolo 2 (RICHIESTA DEL CLIENTE), al termine dell'attività sarà fornito un report che conterrà:

a. Topologia rilevata

b. Descrizione del metodo e degli strumenti

c. Elenco delle vulnerabilità riscontrate e relative contromisure

d. L'elenco dei sistemi/apparati acceduti in modo non autorizzato

e. Eventuali esempi delle informazioni ottenute

Sarà inoltre allegata una descrizione dei possibili miglioramenti che potrebbero essere applicati alla rete, ai sistemi o 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.

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

5. PIANO DI INTERVENTO

5.1. Attività (tipologie)

Attività
Incontro per la definizione del *boundary* dell'attacco *esterno* (Orari, indirizzi, domini)
Attività di Ethical Hacking
Incontro per la presentazione dei risultati e di tutto il materiale prodotto

5.2. Documenti necessari

Per dare inizio alle attività sarà necessaria la sottoscrizione dei due allegati:

- Allegato A: Liberatoria
- Allegato B: Accordo di Non Divulgazione

6. 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 l'eventuale 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.

7. OFFERTA ECONOMICA

7.1. Servizi

Servizi	Costo a corpo
Attività di Assessment di rete e applicativa come precedentemente indicato, comprensivo dell'acquisto del software per scanning	**€ 15.000,00**

8. CONDIZIONI GENERALI DI OFFERTA

Validità offerta:	30 gg
Fatturazione:	50% all'ordine - 50% alla consegna dei deliverables
Liquidazione fatture	30 D.F.F.M.
Trasporti	Ns. carico
Garanzia	A norma di legge

Tutti i prezzi esposti nella presente offerta sono da intendersi IVA esclusa.