]HackingTeam[

Milano, 20 Marzo 2006

Spett.le
Cassa di Risparmio di Bolzano
Via Orazio, 4/D
39100 Bolzano

Offerta n. 20060320.mb16

Alla cortese attenzione: Dott. Claudio Biasin

Oggetto: Offerta per attività di Vulnerability Assessment su Portale Internet Banking

A seguito dei colloqui intercorsi 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

Titolo documento:	*Tipo documento:*	*Versione*:
Ethical Hacking 20060320.mb16	**Offerta**	1.0

Offerta per Attività di Vulnerability Assessment Su Portale di Internet Banking di Cassa di Risparmio di Bolzano

SOMMARIO

1. STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	20 Marzo 2006	Emissione

2. RICHIESTA DEL CLIENTE

Il Cliente richiede di formulare una proposta, con relativa offerta economica, relativa ad interventi di Ethical Hacking sulla rete e i sistemi che compongono il Portale di Internet Banking.

In altre parole, si richiede una consulenza di security assessment che verifichi, secondo una logica indipendente e supra partes, l'effettiva sicurezza della rete, a fronte di attacchi provenienti da Internet, e attacchi diretti alle applicazioni web esposte in Internet.

Più precisamente, il dimensionamento delle attività e' il seguente:

- Attività di Ethical Hacking dall'esterno su rete e sistemi.

  Verranno testati gli indirizzi IP della rete del Cliente sui quali sono attestati i sistemi ospitanti l'Internet Banking.

- Attività di Ethical Hacking a livello applicativo di servizi web

  Verranno testate le applicazioni web, composte da form di login e form generiche, utilizzate per erogare il servizio di Internet Banking.

Il cliente specifica, inoltre, che i seguenti punti devono essere compresi nei risultati della consulenza in oggetto:

- Documento tecnico che riporti le vulnerabilità individuate e i passi necessari per eliminarle.
- Executive Summary per il management
- Presentazione al management

3. DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA

3.1. 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 sia con approccio “black box” (senza credenziali utente) che “white box” con credenziali fornite dal Cliente.

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,

[1] Vogliamo specificare che, considerata la natura della presente offerta, le nostre attività *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 cercherà di **dimostrare l'effettiva possibilità di assumere il controllo dei sistemi senza apportare alcuna modifica agli stessi.**

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.

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

Questa analisi è costituita da una serie di tentativi di attacco che coinvolgono solo i protocolli di comunicazione utilizzati dagli utenti finali per interagire con le applicazioni. Nel caso specifico delle applicazioni web, tali attacchi sono basati su manipolazioni dei pacchetti HTTP che vengono scambiati fra i browser degli utenti ed il web server. Esistono diverse categorie di attacchi

verso applicazioni web, che possono portare alla compromissione di uno o più layer dell'intera infrastruttura applicativa: web server, application server, data tier.

Caratteristica comune a tutti gli attacchi applicativi è la completa trasparenza ad ogni sistema di difesa perimetrale (firewall, ids, ecc.): manipolazioni dei protocolli di layer 7 (applicativi) non possono essere rilevate da dispostivi che analizzano il traffico a layer 3 (network).

Il test sarà condotto in modalità anonima ed in "user-mode". 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. 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. 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' attivita' di security audit dell' applicazione web identifica in modo completo le classi di attacco, in particolare saranno testate:

- Cross-site scripting: attacchi che sfruttano una non corretta validazione dei contenuti restituiti dal server in risposta a richieste HTTP opportunamente modificate.
- Parameter tampering: attacchi che sfruttano una non corretta validazione dei parametri passati dal browser al web server.
- Hidden field manipulation: attacchi che, sfruttando paradigmi di programmazione non sicuri, alterano il valore di parametri applicativi fra due successive richieste HTTP.
- Backdoors e opzioni di debug: attacchi basati su errori di configurazione e/o di programmazioni molto noti e diffusi.
- Stealth commanding: attacchi che mediante tecniche di injection mirano ad eseguire comandi sui server.

- Forceful browsing: attacchi che mirano ad accedere a risorse protette seguendo percorsi di navigazione non previsti.
- Buffer overflow: attacchi che comportano l'esecuzione di codice arbitrario in assenza di opportuna validazione dei parametri in ingresso.
- Cookie poisoning: attacchi basati sulla manipolazione dei cookie di sessione HTTP.
- Configurazioni errate: attacchi che sfruttano comuni errori di configurazione.
- Vulnerabilità note: attacchi che sfruttano la mancata applicazione di patch.
- SQL injection: attacchi che mirano all'esecuzione di query non previste sui DBMS di backend
- Attacchi http: manipolazioni degli Header 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. Dettagliata descrizione del metodo e degli strumenti
c. L'elenco dei sistemi/apparati acceduti in modo non autorizzato
d. Descrizione della catena di eventi che hanno portato all'accesso della rete/sistema/applicazione
e. Log degli eventi
f. 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.

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

Le attività verranno svolte durante l'orario notturno (21.00 – 06.00) dai laboratori Hacking Team.

Si richiede di poter pianificare i tempi dei tentativi di attacco in modo da consentire al Cliente di seguire le attività sui target e di accorgersi tempestivamente di eventuali disservizi.

In ogni caso, le attività verranno condotte minimizzando le attività di DoS.

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'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

Descrizione Servizi	Costo
Attività di Vulnerability Assessment a livello sistemi e applicativo sul Servizio di Internet Banking	€ 11.500,00
Quotazione a Voi riservata	**€ 9.300,00**

Il completamento delle attività di assessment è previsto, comprendendo la stesura della documentazione finale, in un arco temporale di circa 20 giorni solari.

7.2. Documentazione Utente

La documentazione e la reportistica sono comprese nei servizi sopra esposti.

8. CONDIZIONI GENERALI DI OFFERTA

Validità offerta:	30 gg
Fatturazione:	50% all'ordine 50% all 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.