]HackingTeam[

Milano, 24 Novembre 2005

Spett.le
**Barclays Bank PLC**
Via Pantano, 13
20122 Milano (MI)

Offerta n. 20051124.mb47

**Alla cortese attenzione: Dr. Gianpiero Acerbi**

**Oggetto: Offerta per attività di Security Assessment**

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

| *Titolo documento:* | *Tipo documento:* | *Versione*: |
|---|---|---|
| **Offerta Barclays VA e PT 20051124.mb47** | **Offerta** | 1.0 |

# Offerta per attività di Vulnerability Assessment e Penetration Test

# SOMMARIO

**1. STORIA DEL DOCUMENTO ..... 4**

**2. RICHIESTA DEL CLIENTE ..... 5**

**3. DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA ..... 6**

3.1. SECURITY PROBE ..... 6

**4. DOCUMENTAZIONE UTENTE ..... 8**

**5. PIANO DI INTERVENTO ..... 9**

5.1. ATTIVITÀ (TIPOLOGIE) ..... 9
5.2. DOCUMENTI NECESSARI ..... 9

**6. RESPONSABILITÀ ..... 10**

**7. OFFERTA ECONOMICA ..... 11**

7.1. SERVIZI ..... 11
7.2. DOCUMENTAZIONE UTENTE ..... 11
7.3. PIANO DI MANUTENZIONE ..... 11

**8. CONDIZIONI GENERALI DI OFFERTA ..... 11**

# 1. STORIA DEL DOCUMENTO

| Versione: | Data: | Modifiche effettuate: |
|---|---|---|
| 1.0 | 24 Novembre 2005 | Emissione Offerta |

## 2. RICHIESTA DEL CLIENTE

Barclays Bank richiede di formulare una proposta, con relativa offerta economica, relativa ad interventi di Ethical Hacking sulle policy, sulla rete e i sistemi della propria infrastruttura.

Le attività richieste sono:

- Vulnerability Assessment e Penetration Test dei sistemi della rete interna (circa 150 server e 300 client)

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

- Verifica con relativo report sui permessi relativi alle cartelle dei file server e alle condivisioni di rete (circa 7 dischi condivisi su 4 file server)
- Verifica sullo stato di aggiornamento dei sistemi client e server (sia fisici che virtuali)
  - Sistema operativo installato sulla macchina e lista di patch e service packs installate
  - Applicazioni installate sulla macchina e lista di patch e service packs installate
- Verifica delle policy di sicurezza riguardo agli accessi terminal server (circa 7 server da verificare sulle policy di dominio)
- Verifica della configurazione dei prodotti antivirus installati sulle macchine e stato di aggiornamento delle segnature (il sistema utilizzato è Norton ed è gestito centralmente attraverso una GUI di management)
- Verifica della configurazione dei firewall Checkpoint (un cluster checkpoint con circa 50 regole di policy)
- Port scanning sulla rete interna
- Penetration test sui router (di proprietà del cliente)
- Verifica della configurazione del sistema IDS (policy di configurazione)
- Verifica della configurazione degli switch (di proprietà del cliente)

- Verifica della sicurezza sui sistemi di accesso remoto alla LAN aziendale (VPN con strong authentication e VPN SSL)
- Verifica della sicurezza della web mail
- Analisi della configurazione degli accessi ai server applicativi (si ipotizzano circa 30 server)

# 3. DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA

## 3.1. Security Probe

Per tutte le attività richieste che riguardano azioni di hacking etico per la verifica della sicurezza, verrà adottata la metodologia seguente.

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 sia esso su internet che sulla rete interna.

Hacking Team propone e realizza questi servizi da quasi dieci anni, prima all'interno di altre organizzazioni e dal 2003 in proprio.

Sul sito www.hackingteam.it sono riportate le numerose referenze presso istituzioni bancarie e altri settori.

### 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 sia internamente che 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", 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, ethercap).

## 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" nei sistemi sotto test. 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 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.

## 3.2. Esame vulnerabilità ambienti server e client

Oltre a tecniche di attacco specifiche per verificare le vulnerabilità riscontrate, verranno utilizzati componenti che consentono di raccogliere le informazioni dai sistemi sotto analisi.

In particolare, per ciò che riguarda livelli di service pack, patch, antivirus e programmi installati, verrà utilizzato un modulo di nostra proprietà che eseguirà un censimento di tutti gli asset aziendali e fornirà il loro livello di sicurezza in riferimento alle security policy definite dal Cliente.

L'output di questa analisi sarà molto importante per definire il gap tra la situazione attuale e quella attesa.

Verranno inoltre analizzate le configurazioni presenti su switch, IDS e firewall per comprenderne il livello di adeguatezza.

# 4. DOCUMENTAZIONE CONSEGNATA

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

- **Descrizione dei sistemi analizzati**
- **Descrizione del metodo, delle attività eseguite e degli strumenti utilizzati**
- **Report sui permessi dei file system condivisi**

[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.**

- **Report sul port scanning effettuato**
- **Gli obiettivi di sicurezza che si vogliono raggiungere (definiti insieme al cliente)**
- **Gap Analysis**
- **Elenco delle vulnerabilità riscontrate e relative contromisure rispetto agli obiettivi di sicurezza che si vogliono raggiungere**
- **Considerazioni finali**
- **Executive summary e documento di presentazione per il management in forma di slides**

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* delle attività (Orari, indirizzi, domini) e delle architetture, reti e sistemi da verificare |
| Attività di Ethical Hacking interno su router, webmail |
| Attività di Scanning sulla rete interna |
| Analisi delle policy e delle configurazioni secondo quanto indicato nelle richieste del cliente (capitolo 2) |
| Analisi dell'accesso condiviso dei dischi di rete |
| Verifica del livello di aggiornamento del software |
| Stesura e consegna documentazione come sopra descritta |
| 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 |
|---|---|
| **Assessment di security (tutte le attività elencate nella tabella sopra descritta)** | **€ 41.500,00** |

## 7.2. Documentazione

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

## 7.3. Piano di manutenzione

In questa offerta non e' previsto piano di manutenzione.

# 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.