

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Galbusera 20070112.03GP	Offerta	1.0

Milano, 12 gennaio 2007

Spett.le
Galbusera S.p.A.
Via Orobie, 9
16122 Cosio Valtellino (SO)

Offerta n. 20070112.03GP

Alla cortese attenzione: Sig. Dante Gelmini

Oggetto: Offerta per attività Ethical Hacking – livello applicativo web

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.
Gabriele Parravicini
Responsabile commerciale



Data documento: 12 gennaio 2007	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20070112.03GP	Pagina: 1 di 11
------------------------------------	---------------------------------	---------------------------------	--	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Galbusera 20070112.03GP	Offerta	1.0

Offerta Ethical Hacking – Galbusera

Data documento: 12 gennaio 2007	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20070112.03GP	Pagina: 2 di 11
------------------------------------	---------------------------------	---------------------------------	--	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Galbusera 20070112.03GP	Offerta	1.0

SOMMARIO

STORIA DEL DOCUMENTO	4
RICHIESTA DEL CLIENTE	5
SOLUZIONE PROPOSTA	5
DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA	6
SECURITY PROBE	6
Analisi non invasiva	6
Analisi invasiva	7
Attacco.....	7
Consolidamento.....	8
DOCUMENTAZIONE UTENTE	8
PIANO DI INTERVENTO	9
ATTIVITÀ (TIPOLOGIE).....	9
DOCUMENTI NECESSARI.....	9
RESPONSABILITÀ	9
OFFERTA ECONOMICA	10
SERVIZI.....	10
DOCUMENTAZIONE UTENTE	10
PIANO DI MANUTENZIONE.....	10
TOTALE A VOI RISERVATO	10
CONDIZIONI GENERALI DI OFFERTA	11

Data documento: 12 gennaio 2007	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20070112.03GP	Pagina: 3 di 11
------------------------------------	---------------------------------	---------------------------------	--	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Royal & SunAlliance S.p.A. 20061122.15GP	Offerta	1.0

STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	12 gennaio 2007	Emissione

Data documento: 22 novembre 2006	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061122.15GP	Pagina: 4 di 11
-------------------------------------	---------------------------------	---------------------------------	--	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Royal & SunAlliance S.p.A. 20061122.15GP	Offerta	1.0

RICHIESTA DEL CLIENTE

Galbusera S.p.A. richiede di formulare una proposta, con relativa offerta economica, relativa ad interventi di Ethical Hacking sui propri indirizzi IP esposti alla rete pubblica.

In altre parole, si richiede una consulenza di security assessment che verifichi, secondo una logica indipendente e supra partes, l'*effettiva* sicurezza dei sistemi esposti alla rete pubblica.

Il dimensionamento delle attività e' il seguente:

- Attività di Ethical Hacking a livello reti e sistemi che abbia origine da Internet su 2 IP pubblici

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.
- Documento di presentazione per il management in forma di *slides*
- Presentazione di quest'ultimo punto al management

SOLUZIONE PROPOSTA

L'intervento proposto si compone delle seguenti parti:

- Ethical Hacking dall' esterno:
 - Verifica della sicurezza simulando un attacco che origini da Internet.
 - Verifica della sicurezza approfondendo e combinando le fasi di Ethical Hacking precedenti. Si tratta della fase di maggiore importanza, in quanto si cerca di "sommare" le vulnerabilità eventualmente trovate per penetrare ancora più in profondità nel sistema. In questa fase vengono usati esclusivamente strumenti *custom*, cioè sviluppati *ad hoc* per il cliente e/o proprietari. Alcuni risultati di questa fase possono essere: cattura parole chiave, intrusione/accesso interattivo non autorizzato, controllo procedure

Data documento: 22 novembre 2006	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061122.15GP	Pagina: 5 di 11
-------------------------------------	---------------------------------	---------------------------------	--	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Royal & SunAlliance S.p.A. 20061122.15GP	Offerta	1.0

interne, accesso a dati personali, accesso a sistemi secondari e/o paralleli, *escalation dell'attacco a vari livelli.*

DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA

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 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) ed, infine, quali sistemi operativi "posseggano". Gli strumenti utilizzati sono: interrogazioni ICMP (gping, fping, ecc.), scansione delle porte TCP e UDP (strobe, netcat, nmap, ecc.), fingerprint dello stack (nmap, ethercap).

Data documento: 22 novembre 2006	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061122.15GP	Pagina: 6 di 11
-------------------------------------	---------------------------------	---------------------------------	--	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Royal & SunAlliance S.p.A. 20061122.15GP	Offerta	1.0

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 PRIVILEGES¹

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

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**.

Data documento: 22 novembre 2006	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061122.15GP	Pagina: 7 di 11
-------------------------------------	---------------------------------	---------------------------------	--	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Royal & SunAlliance S.p.A. 20061122.15GP	Offerta	1.0

(/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.

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**

Data documento: 22 novembre 2006	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061122.15GP	Pagina: 8 di 11
-------------------------------------	---------------------------------	---------------------------------	--	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Royal & SunAlliance S.p.A. 20061122.15GP	Offerta	1.0

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.

PIANO DI INTERVENTO

Attività (tipologie)

Attività
Incontro per la definizione del <i>boundary</i> dell'attacco <i>esterno</i> (Orari, indirizzi, domini)
Attività di Ethical Hacking dall'esterno
Incontro per la presentazione dei risultati e di tutto il materiale prodotto: <ul style="list-style-type: none">• Report Direzionale.• Report tecnico dettagliato con indicazione delle possibili soluzioni.

Documenti necessari

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

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

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.

Data documento: 22 novembre 2006	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061122.15GP	Pagina: 9 di 11
-------------------------------------	---------------------------------	---------------------------------	--	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Royal & SunAlliance S.p.A. 20061122.15GP	Offerta	1.0

OFFERTA ECONOMICA

Servizi

Servizi	Descrizione	Costo
Ethical Hacking applicativo (Esterno)	Ethical Hacking dall'esterno	€2.500,00

Documentazione Utente

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

Piano di manutenzione

In questa offerta non e' previsto piano di manutenzione.

Totale a voi riservato

Servizi	Descrizione	Costo a voi riservato
Ethical Hacking applicativo (Esterno)	Ethical Hacking dall'esterno	€1.200,00

I costi indicati si intendono al netto delle imposte.

Data documento: 22 novembre 2006	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061122.15GP	Pagina: 10 di 11
-------------------------------------	---------------------------------	---------------------------------	--	---------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Royal & SunAlliance S.p.A. 20061122.15GP	Offerta	1.0

CONDIZIONI GENERALI DI OFFERTA

Modalità di pagamento e condizioni generali di fornitura

Validità offerta:	30 gg
Pagamenti	All'ordine
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.

Data documento: 22 novembre 2006	Autore: Gabriele Parravicini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061122.15GP	Pagina: 11 di 11
-------------------------------------	---------------------------------	---------------------------------	--	---------------------