

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04 GP	Offerta	1.0

Milano, 19 giugno 2007

Spett.le
Axa Assicurazioni S.p.A.
Via Leopardi, 15
20100 Milano (MI)

Offerta n. 20070619.04GP

Alla cortese attenzione: Dott. Matteo Feraboli

Oggetto: Offerta per attività Ethical Hacking – applicativo

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: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadruccio	Codice documento: OFF-20070619.04 GP	Pagina: 1 di 13
-----------------------------------	---------------------------------	---------------------------------	-----------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04 GP	Offerta	1.0

Offerta Ethical Hacking – Axa Assicurazioni

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadruccio	Codice documento: OFF-20070619.04 GP	Pagina: 2 di 13
-----------------------------------	---------------------------------	---------------------------------	-----------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04 GP	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
ANALISI APPLICATIVA	9
SOURCE CODE REVIEW	10
DOCUMENTAZIONE UTENTE	11
PIANO DI INTERVENTO	11
ATTIVITÀ (TIPOLOGIE).....	11
DOCUMENTI NECESSARI.....	12
RESPONSABILITÀ	12
OFFERTA ECONOMICA	12
SERVIZI.....	12
DOCUMENTAZIONE UTENTE	12
PIANO DI MANUTENZIONE.....	12
COSTO A VOI RISERVATO	13
CONDIZIONI GENERALI DI OFFERTA	13

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadruccio	Codice documento: OFF-20070619.04 GP	Pagina: 3 di 13
-----------------------------------	---------------------------------	---------------------------------	-----------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	19 giugno 2007	Emissione

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadrucchio	Codice documento: OFF-200706219.04GP	Pagina: 4 di 13
-----------------------------------	---------------------------------	----------------------------------	-----------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

RICHIESTA DEL CLIENTE

Axa Assicurazioni richiede di formulare una proposta, con relativa offerta economica, relativa ad interventi di Ethical Hacking sul proprio applicativo sinistri.

In altre parole, si richiede una consulenza di security assessment che verifichi, secondo una logica indipendente e supra partes, l'*effettiva* sicurezza del proprio applicativo per la gestione dei sinistri.

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

- Attività di Ethical Hacking di rete e sistemistica ed applicativa sull'infrastruttura dell'applicativo sinistri con approccio black box.
- Attività di Ethical Hacking a livello applicativo con approccio white box.
- Source code auditing al fine di individuare problematiche di sicurezza derivanti dalla programmazione dell'applicativo.

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 black box:
 - Verifica della sicurezza simulando un attacco alla rete, ai sistemi ed all'applicativo senza essere in possesso di credenziali utente.
- Ethical Hacking white box:
 - Verifica della sicurezza simulando attacchi applicativi essendo in possesso delle credenziali utente;
 - Verifica della sicurezza approfondendo e combinando le fasi di Ethical Hacking precedenti. Si tratta della fase di maggiore importanza, in quanto si

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadrucchio	Codice documento: OFF-200706219.04GP	Pagina: 5 di 13
-----------------------------------	---------------------------------	----------------------------------	-----------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

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 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) e, infine, quali sistemi operativi “posseggano”.

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadrucchio	Codice documento: OFF-200706219.04GP	Pagina: 6 di 13
-----------------------------------	---------------------------------	----------------------------------	-----------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

Gli strumenti utilizzati sono: interrogazioni ICMP (gping, fping, 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” 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.

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadrucchio	Codice documento: OFF-200706219.04GP	Pagina: 7 di 13
-----------------------------------	---------------------------------	----------------------------------	-----------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

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 (/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.

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: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadrucchio	Codice documento: OFF-200706219.04GP	Pagina: 8 di 13
-----------------------------------	---------------------------------	----------------------------------	-----------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

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 dispositivi 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'attività 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 parametric passati dal browser al web server.

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadrucchio	Codice documento: OFF-200706219.04GP	Pagina: 9 di 13
-----------------------------------	---------------------------------	----------------------------------	-----------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

- 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.
- Vulnerabilita' 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.

SOURCE CODE REVIEW

In questa fase verrà analizzato il codice sorgente dell'applicativo al fine di verificare la presenza di eventuali errori in fase di programmazione che compromettano e pregiudichino la sicurezza dell'applicativo stesso.

Ci si concentrerà in particolare sull'analisi delle form di autenticazione non trascurando però la struttura vera e propria del target dell'attività.

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadruccio	Codice documento: OFF-200706219.04GP	Pagina: 10 di 13
-----------------------------------	---------------------------------	---------------------------------	-----------------------------------------	---------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

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.

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
Attività di Ethical Hacking sistemistico dall'interno
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.

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadrucchio	Codice documento: OFF-200706219.04GP	Pagina: 11 di 13
-----------------------------------	---------------------------------	----------------------------------	-----------------------------------------	---------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

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 iniziale, 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.

OFFERTA ECONOMICA

Servizi

Servizi	Descrizione	Costo
Ethical Hacking	Security probe	€ 20.000,00

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.

Data documento: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadrucchio	Codice documento: OFF-200706219.04GP	Pagina: 12 di 13
-----------------------------------	---------------------------------	----------------------------------	-----------------------------------------	---------------------

Titolo documento:	Tipo documento:	Versione:
Ethical Hacking Axa Assicurazioni 20070619.04GP	Offerta	1.0

Costo a voi riservato

Servizi	Descrizione	Costo
Ethical Hacking	Security probe	€17.500,00

I costi indicati si intendono al netto delle imposte.

CONDIZIONI GENERALI DI OFFERTA

Modalità di pagamento e condizioni generali di fornitura

Validità offerta:	30 gg
Fatturazione servizi	50% all'ordine – 50% a fine lavori
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: 19 giugno 2007	Autore: Gabriele Parravicini	Revisore: Gianluca Vadruccio	Codice documento: OFF-200706219.04GP	Pagina: 13 di 13
-----------------------------------	---------------------------------	---------------------------------	-----------------------------------------	---------------------