

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda- 20080306 AL	Offerta	1.0

Milano, 6 Marzo 2008

Spett.le
Cartiere del Garda
Viale Rovereto 15
Riva del Garda

Offerta n. 20080306 AL

Alla cortese attenzione: Sigg. Flavio Tonidandel, Alessandro Avancini

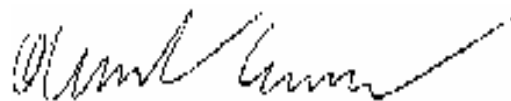
Oggetto: Offerta per attività Ethical Hacking

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.

HT Srl

Alessandro Lomonaco



Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 1 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda- 20080306 AL	Offerta	1.0

Offerta Ethical Hacking

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 2 di 15
---	---------------------------------------	------------------	---	---------------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda– 20080306 AL	Offerta	1.0

SOMMARIO

STORIA DEL DOCUMENTO	4
RICHIESTA DEL CLIENTE	5
SOLUZIONE PROPOSTA	5
DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA	7
SECURITY PROBE	7
Analisi non invasiva	7
Analisi invasiva	8
Attacco.....	8
Consolidamento.....	9
Analisi applicativa	10
DOCUMENTAZIONE UTENTE	12
PIANO DI INTERVENTO	13
ATTIVITÀ (TIPOLOGIE).....	13
DOCUMENTI NECESSARI.....	13
RESPONSABILITÀ	14
DOCUMENTAZIONE UTENTE	14
PIANO DI MANUTENZIONE.....	14
OFFERTA ECONOMICA	15
TOTALE A VOI RISERVATO	15
CONDIZIONI GENERALI DI OFFERTA	15

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 3 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda- 20080306 AL	Offerta	1.0

STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	06 Marzo 2008	Emissione

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 4 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda– 20080306 AL	Offerta	1.0

RICHIESTA DEL CLIENTE

Cartiere del Garda richiede di formulare una proposta, con relativa offerta economica, relativa ad interventi di Ethical Hacking sulla propria rete.

In altre parole, si richiede una consulenza di security assessment che verifichi, secondo una logica indipendente e supra partes, l'effettiva sicurezza della rete, degli applicativi dell'infrastruttura informativa di Cartiere del Garda.

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

- Attività di Ethical Hacking a livello perimetrale. Saranno "testati" gli indirizzi IP del perimetro della rete Cartiere del Garda. (**Modulo 1 dell'attività**)
- Attività di Ethical Hacking applicativo sul sito web di Cartiere del Garda. (**Modulo 2 dell'attività**)
- Attività di Ethical Hacking sull'infrastruttura VPN di Cartiere del Garda. (**Modulo 3 dell'attività**)

SOLUZIONE PROPOSTA

L'intervento proposto si compone delle seguenti parti:

- Ethical Hacking dall' esterno:
 - Verifica della sicurezza simulando un attacco che origini da Internet.
- Ethical Hacking sistemistico ed applicativo:
 - Verifica della sicurezza simulando attacchi sistemistici ed applicativi;
 - Verifica della sicurezza approfondendo e combinando le fasi di Ethical Hacking precedenti. Si tratta della fase di maggiore importanza, in quanto si

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 5 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda– 20080306 AL	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*.

- Ethical Hacking VPN Client :

Verifica della sicurezza delle connessioni VPN Client.

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 6 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda– 20080306 AL	Offerta	1.0

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". 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: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 7 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda– 20080306 AL	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

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: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 8 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda- 20080306 AL	Offerta	1.0

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.

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 9 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	--------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda– 20080306 AL	Offerta	1.0

Analisi applicativa

Questa analisi è costituita da una serie di tentativi d' 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 parametri passati dal browser al web server.

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 10 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	---------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda– 20080306 AL	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.

Precisazioni:

- Nel caso in cui il test avvenga su ambienti in produzione occorre utilizzare, ove possibile, un account di test creato appositamente per la scansione.
- Per tale account devono valere le seguenti condizioni:
 - Accesso esclusivamente riservato a record di test nei database di back-end,
 - Ordini di acquisto o altre tipologie di transazioni dovrebbero essere ignorati,
 - Eventuali nuovi record creati da tale account devono essere successivamente cancellati,
 - Qualora le transazioni abbiano un qualche tipo di impatto (per esempio in caso di acquisto/vendita di azioni), il loro effetto dovrebbe riguardare esclusivamente dei record di test.

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 11 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	---------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda- 20080306 AL	Offerta	1.0

- Qualora l'applicazione preveda diversi livelli di privilegio, è consigliabile effettuare un'analisi con un numero di credenziali di test pari al numero dei profili esistenti e previsti.
- E' consigliabile preventivare e tenere in considerazione il tempo necessario allo sviluppo di script/procedure di clean-up per ripulire tutti i dati creati/modificati dall'utente di test.
- E' utile identificare e comunicare eventuali script o parametri che invalidino le sessioni al fine di evitare che durante le scansioni tali script o parametri vengano eseguiti dai tool di test automatizzati.
- Unitamente alla documentazione dell'analisi verrà rilasciato l'elenco delle URL sottoposte a scansione.

DOCUMENTAZIONE UTENTE

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.

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 12 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	---------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda- 20080306 AL	Offerta	1.0

PIANO DI INTERVENTO

Attività (tipologie)

Attività
Attività di Ethical Hacking dall'esterno
Attività di Ethical Hacking applicativo
Attività di Ethical Hacking VPN client

Documenti necessari

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

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

Data documento: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 13 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	---------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda– 20080306 AL	Offerta	1.0

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.

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: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 14 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	---------------------

Titolo documento:	Tipo documento:	Versione:
Cartiere del Garda- 20080306 AL	Offerta	1.0

OFFERTA ECONOMICA

Totale a voi riservato

Servizi	Descrizione	Costo
Ethical Hacking	Ethical Hacking dall'esterno	3.500,00
Ethical Hacking	Ethical Hacking applicativo	4.900,00
Ethical Hacking	Ethical Hacking VPN Client	2.100,00

I costi indicati si intendono al netto delle imposte e dei costi di trasferta.

CONDIZIONI GENERALI DI OFFERTA

Modalità di pagamento e condizioni generali di fornitura

Validità offerta:	30 gg
Fatturazione servizi	all'ordine
Spese di trasferta	Piè di lista – max 150,00 € per persona al giorno
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: 06 Marzo 2008	Autore: Alessandro Lomonaco	Revisore:	Codice documento: OFF-20080306.AL	Pagina: 15 di 15
----------------------------------	--------------------------------	-----------	--------------------------------------	---------------------