Milano, 25 Luglio 2008

Spett.le

UBI CENTROSYSTEM
Viale Monza 265
20126 Milano

Offerta n. 20080724.083-1.IR

Alla cortese attenzione: Dr. Emilio Segala, Dr. Luigi Chionsini, Dr. Davide Biscaro

Oggetto: Offerta per attività di 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.

Hacking Team Srl

Ivan Roattino

Offerta
Ethical Hacking – UBI CENTROSYSTEM

SOMMARIO

STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	24 Luglio 2008	Emissione

RICHIESTA DEL CLIENTE

UBI CS richiede di formulare una proposta, con relativa offerta economica per 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 del network , degli applicativi Web e della rete interna.

SOLUZIONE PROPOSTA

L'intervento proposto comprende:

- Attività di Ethical Hacking network da esterno relativa a 64 indirizzi IP
- Attività di Ethical Hacking da interno presso sedi di Ubi CS
  (CED di Assago o sede di Viale Monza 265- Milano) su nr. 250 server.
- Attività di Ethical Hacking applicativo su nr. 38 applicazioni web
  (come da elenco incluso alla presente offerta)

.

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. Di seguito sono riportate le metodologie rispettivamente per la verifica network dall'esterno, per la verifica applicativa. Esse contemplano un livello di approfondimento notevole.

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).

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, per

[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.**

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 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 dispostivi che analizzano il traffico a layer 3 (network).

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 vaidazione dei contenuti restituiti dal server in risposta a richieste HTTP opportunamente modificate.
- Parameter tampering: attacchi che sfruttano una non corretta vaidazione dei parametric 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 manipoloazione dei coockie 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.

DOCUMENTAZIONE UTENTE

Oltre a ciò specificatamente richiesto nel capitolo 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. **Report direzionale**
f. **Log degli eventi**
g. **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
Attività di VULNERABILITY ASSESSMENT network da esterno: Vulnerability Assessment network da esterno con approccio black-box su classe di 64 indirizzi IP. Output: ✓ Descrizione dei test effettuati ✓ Vulnerabilità riscontrate ✓ Strategia di fixing a copertura delle minacce **Attività di VULNERABILITY ASSESSMENT interno**: Vulnerability Assessment con approccio black-box da interno presso Vs. data center sede di Assago su nr. 250 Server Output: ✓ Vulnerabilità macroscopiche riscontrate ✓ Security plan a copertura delle minacce evidenti ✓ Proposta di ulteriori verifiche mirate ed approfondite **Attività di VULNERABILITY ASSESSMENT applicativi**: Web Application Assessment con approccio black-box. Output: ✓ Descrizione dei test effettuati ✓ Vulnerabilità riscontrate ✓ Strategia di fixing a copertura delle minacce ✓ Proposta di ulteriori verifiche mirate ed approfondite

ELENCO APPLICATIVI WEB OGGETTO DI VERIFICA:	
B247	www.bankyou.it
	www.banca247.it
	www.bankyoumutui.it
	www.cartalibra.it
	infp01.cartalibra.it
	mutuiass.banca247.it
	insoluti.bankyou.it
	www.cartakalia.it
	pre.capitalmoney.bpb.it
	capitalmoney.bpb.it
	pre.cartalibra.it
	pre.banca247.it
	webmail.bankyou.it
	hype.bankyou.it
	pre.bankyou.it
	infc01.cartalibra.it
	reports.bankyou.it
	img.bankyou.it
UBI CENTROSYSTEM	www.bpucentrosystem.it
	ftp.bpucentrosystem.it
	supporto.bpucentrosystem.it
	www.finanziariaromana.it
	mail.ubicentrosystem.it
CENTROBANCA	secure.centrobanca.it
UBI ESALEASING	leasingonline.ubicentrosystem.it
	leasingtest.ubicentrosystem.it
UBI PRAMERICA	www.finanzattiva.com
	www.ubipramerica.it
	areariservata.ubiassicurazioni.it
MERCATO IMPRESA	www.coraliscard.it
	creso.coralis.it
	www.cresoclub.com
	duetto.coralis.it
	utilio.coralis.it
	catalogo.coralis.it
	report.coralis.it
	www.coralis.it
UBI SIM	www.ubisimple.it

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 HT 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 HT 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.

OFFERTA ECONOMICA

Totale a voi riservato

Servizi	Descrizione	Costo
Ethical Hacking	**Vulnerability Assessment network da esterno**	**€ 9.000**
	Vulnerability Assessment interno	**€ 15.000**
Ethical Hacking Applicativo	**Vulnerability Assessment applicativo relativo a: (vedi elenco sopra incluso)**	**€ 58.000**

Le spese di trasferta per le attività svolte presso Vs. sedi sono comprese.

CONDIZIONI GENERALI DI OFFERTA

Modalità di pagamento e condizioni generali di fornitura

Validità offerta:	30 gg
Fatturazione servizi	50% all'ordine e 50% a fine lavori
Liquidazione fatture	30 D.F.F.M.
Garanzia	A norma di legge

Tutti i prezzi esposti nella presente offerta sono da intendersi IVA esclusa.