]HackingTeam[

Milano, 4 Gennaio 2007

Spett. le
Fujitsu Siemens

Offerta n. 20070104.mb01

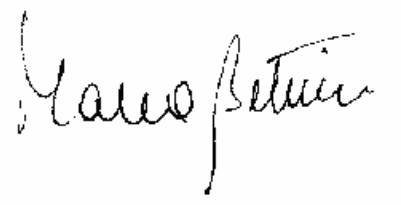
Alla cortese attenzione: Sig. Davide Piva

Oggetto: Offerta per attività di Vulnerability Assessment

A seguito della Vostra gradita richiesta, vi sottoponiamo la nostra proposta per il servizio in oggetto relativo al Cliente Cartiere del Garda.

In attesa di un vostro gradito riscontro, vi porgiamo i nostri più cordiali saluti.

Hacking Team S.r.l.
Marco Bettini
Key account Manager



Hacking Team S.r.l.
Sede legale e Amministrativa: Via Freguglia Carlo, 2– 20122 Milano
Sede operativa: Via della Moscova, 13 - 20121 Milano – Tel: +39.02.29060603
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Offerta per attività di Vulnerability Assessment e Penetration Test

SOMMARIO

1. STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	4 Gennaio 2007	Emissione Offerta

2. RICHIESTA DEL CLIENTE

Siemens Informatica richiede di formulare una proposta, con relativa offerta economica, relativa ad interventi di Ethical Hacking sulla rete, i sistemi e le applicazioni del proprio Cliente Cartiere del Garda.

Le attività richieste sono:

- Vulnerability Assessment e Penetration Test da Internet (16 IP pubblici)
- Vulnerability Assessment e Penetration Test della rete interna e delle applicazioni
- Vulnerability Assessment e Penetration Test applicativo su RAS Server
- Vulnerability Assessment e Penetration Test su due reti wireless (magazzino ed uffici)

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

3. DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA

3.1. Security Probe

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.

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, ettercap).

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.

[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.**

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

L'oggetto di questa parte di attività sarà il tentativo di accesso e di verifica della sicurezza delle applicazioni.

Il test può essere 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 delle applicazioni identifica in modo completo le classi di attacco, in particolare saranno testate:

- Parameter tampering
- Backdoors e opzioni di debug
- Stealth commanding
- Buffer overflow
- DNS Poisoning
- Configurazioni errate
- Vulnerabilità note
- SQL injection

3.2. Assessment Reti Wireless

La possibilità di integrare il wireless alla rete cablata aziendale con una spesa minima rappresenta un'attrazione per molti IT manager. Per contro, il compromesso sta nel fattore sicurezza. Punti di accesso pubblici rendono le reti poco sicure e rappresentano l'anello debole della catena dell'intero network se non si adottano accorgimenti di sorta.

Di conseguenza l'introduzione di infrastrutture Wifi all'interno dell'azienda deve essere accompagnata da una policy di sicurezza forte, mirata a prevenire l'insorgenza di possibili rischi che potrebbero ripercuotersi sull'integrità di tutta la struttura aziendale.

Obiettivo dell'analisi è verificare il grado di sicurezza della rete, le eventuali vulnerabilità dovute ad errate configurazioni

Le fasi previste per l'analisi di sicurezza e penetration test dell'infrastruttura di Rete Wireless sono:

Fase .1. Approccio Black Box

- Network discovery (SSID, IP, Domains)
- Access point mapping
- Analisi traffico
- Analisi cifratura, meccanismo di autenticazione
- Tentativi di accesso AP

- Tentativi Man in the Middle
- Analisi client misconfiguration (rogue access point)

Fase .2. Approccio White Box

- Accesso al network con credenziali low privilege
- IP Network discovery, host/services mapping
- Verifica vulnerabilita' host/services
- Tentativi di accesso a risorse
- Tentativi di override delle politiche di difesa

I rischi

Nella realizzazione dei sistemi wireless, a causa di scelte tecniche non propriamente oculate, si sono venute a delineare alcune debolezze che derivano sia dalla scelta degli standard, sia dalla loro implementazione da parte dei produttori.

Ad alto livello si possono prospettare alcuni scenari di attacco che per praticità potremmo suddividere nelle seguenti categorie:

- attacchi di inserimento
- intercettazione e monitoraggio non autorizzato del traffico
- jamming
- attacchi da client a client
- attacchi brute force all'access point
- attacchi crittografici
- errata configurazione

Capire come funzionano gli attacchi e utilizzare queste informazioni per prevenirli, sono passi fondamentali nella stesura di una policy di sicurezza per una qualsiasi soluzione wireless.

Di seguito vengono riassunte brevemente le caratteristiche delle tipologie di attacco.

Attacchi di inserimento

Consistono nella distribuzione incontrollata e non autorizzata di periferiche wireless e/o sulla creazione di reti wireless abusive, aggirando qualsiasi tipo di revisione architetturale.

In questo caso gli scenari possono essere due:

1. Client non autorizzati: un attaccante tenta di connettersi abusivamente, tramite un notebook all'access point più vicino, in special modo se questi ultimi non sono configurati per richiedere una password all'atto della connessione del client.
2. Access point non autorizzato: questa tecnica prevede l'installazione di 'rogue' access point, punti di connessione clandestini o altamente insicuri, che danno la possibilità di avere accesso alle risorse della rete da client fuori perimetro.

Entrambe le tecniche consentono l'accesso non autorizzato a sistemi wireless, e nel caso peggiore anche la possibilità di raggiungere le risorse aziendale poste sulla rete cablata.

La gravità dell'intrusione é in diretta relazione con il contenuto informativo dei sistemi connessi dal sistema di distribuzione (DS): si parte dalla semplice visione di documenti riservati, fino ad arrivare alla distruzione degli stessi o addirittura al reperimento e diffusione di dati riservati.

Intercettazione e monitoraggio del traffico

Come nelle reti a cavo, è possibile intercettare e monitorare (sniffare) il traffico sulle reti 802.11[x].

Il punto di forza di questo attacco rispetto a un ambiente wired è che l'attaccante non ha bisogno di compromettere un sistema collegato alla rete per depositare un agente o un Trojan che faccia da sniffer.

Tutto quello di cui si ha bisogno è riuscire a raggiungere la portante dei segnali usati dai sistemi Wifi. Visto che il segnale viene distribuito in maniera circolare sui tre assi dimensionali, il risultato è che questo può essere intercettato da posizioni esterne all'azienda o da un piano all'altro del palazzo.

L'analisi passiva del traffico e/o la clonazione di un Access Point, se non venissero adottate precise contromisure, potrebbero consentire la visione del traffico non cifrato tra utenti e servizi o il reperimento di credenziali di accesso ai sistemi applicativi dell'azienda.

Jamming

Gli attacchi di tipo Denial of Service possono essere facilmente applicati all'ambiente wireless: in questo caso la connettività è compromessa con l'iniezione di traffico illegittimo o disturbo della frequenza di trasmissione.

Un bravo attaccante con un buon equipaggiamento, potrebbe 'inondare' (flooddare) il segnale, corrompendo lo stream dati fino alla caduta del servizio.

Attacchi da client a client

Gli standard prevedono che due client wireless possano colloquiare direttamente tra loro, senza utilizzare l'access point del loro Service Set. Di conseguenza gli utenti, hanno bisogno di essere protetti non solo dai rischi esterni, ma anche da elementi sconosciuti.

Le risorse condivise e i servizi messi a disposizione sulla rete Wifi divengono oggetto di possibili attacchi, come se fossero posti su di una normale rete cablata; attacchi che vanno dal semplice DoS, fino ad attacchi evoluti che consentono di prendere il controllo dei sistemi e delle informazioni in esso residenti.

Attacchi Brute Force vs. access point

Diversi sistemi di distribuzione usano una singola chiave o password per autenticare tutti i client.

Il brute forcing, tramite dizionario o tentativi sequenziali, consente l'accesso al dispositivo di accesso ed di ottenere comodamente tutti i dati utente. Attacchi di questo tipo sono molto diffusi e di grande impatto, sopratutto in ambienti in cui le infrastrutture sono complesse ed eterogenee.

Questi fattori spingono gli amministratori di sistema ad adottare politiche di sicurezza lascive a vantaggio della interoperatività e della semplicità di gestione.

Attacchi crittografici

Lo standard 802.11b usa un sistema di autenticazione chiamato WEP. Questo standard è potenzialmente soggetto a diversi tipi di attacco:

- passivo, basato su analisi statistica del traffico
- attivo, con iniezione di nuovo traffico da una stazione non autorizzata, basato sull'analisi del testo in chiaro passante
- attivo, basato sulla compromissione dell'access point
- attivo, tramite il monitoraggio continuato del traffico in un certo lasso temporale dell'ordine di qualche giorno, permettendo la decifrazione in tempo reale di tutto il traffico

Sia la versione 40bit che la 128bit sono soggette a questi attacchi.

L'invito è di considerare altamente insicuro lo standard WEP e di integrare soluzioni per la sicurezza dell'infrastruttura aggiuntive o standard che utilizzano sistemi di integrità e cifratura più evoluti.

Errata configurazione

Di solito i sistemi di accesso vengono distribuiti con una configurazione standard per una facile messa in produzione ed un utilizzo immediato.

Visto l'obiettivo di avere un apparato pronto all'uso e utilizzabile nei più disparati ambienti, di solito porta a definire configurazioni di default in cui la sicurezza viene posta in secondo piano.

Gli amministratori dovrebbero considerare i rischi che comporta l'utilizzo di questa configurazione , prima di procedere all'installazione, onde evitare di esporre i sistemi ospiti a rischi inutili.

4. 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. Elenco delle vulnerabilità riscontrate e relative contromisure

d. L'elenco dei sistemi/apparati acceduti in modo non autorizzato

e. Descrizione della catena di eventi che hanno portato all'accesso della rete/sistema/applicazione

f. Eventuali esempi delle informazioni ottenute

Sarà inoltre allegata una breve 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.

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* dell'attacco *esterno* (Orari, indirizzi, domini)
Attività di Ethical Hacking
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
Vulnerability Assessment e Penetration Test da Internet	**€ 5.000,00**
Vulnerability Assessment e Penetration Test della rete interna e delle applicazioni	**€ 7.000,00**
Vulnerability Assessment e Penetration Test applicativo su RAS Server	**€ 1.800,00**
Vulnerability Assessment e Penetration Test su due reti wireless (magazzino ed uffici)	**€ 6.500,00**

Le quotazioni sopra indicate si riferiscono ad attività singole. Nel caso il cliente scegliesse di ordinare tutte le attività quotate, il costo globale sarebbe di **€ 17.500,00**.

Non avendo dettagliate informazioni sul boundary da analizzare, il costo sopra riportato è basato su una stima di impegno per l'attività di vulnerability assessment di applicazioni intranet di medie dimensioni.

7.2. Documentazione Utente

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

8. CONDIZIONI GENERALI DI OFFERTA

Validità offerta:	30 gg
Fatturazione:	• 50% alla riunione di startup • 50% alla consegna dei deliverables
Liquidazione fatture	60 D.F.F.M.
Trasporti	Ns. carico
Garanzia	A norma di legge

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