Milano, 11 Luglio 2008

Spett.le
UBI SISTEMI E SERVIZI
Via Cefalonia, 62
25124 BRESCIA

Offerta n. 20080711.078-1.IR

Alla cortese attenzione: Dr. Paolo Colombini

Oggetto: Offerta VA / PENTEST

A seguito dell'incontro intercorso, Vi sottoponiamo la nostra proposta per i servizi in oggetto.

In attesa di un Vostro gradito riscontro, Vi porgiamo i nostri più cordiali saluti.

HT Srl

Ivan Roattino

Offerta
Ethical Hacking – UBI SISTEMI E SERVIZI

SOMMARIO

STORIA DEL DOCUMENTO **4**

1.RICHIESTA DEL CLIENTE **5**

2.SOLUZIONE PROPOSTA **5**

3.METODOLOGIA DELLA SOLUZIONE PROPOSTA **7**

- PREMESSA 7
- I RISCHI 7
- ATTACCHI DI INSERIMENTO 8
- INTERCETTAZIONE E MONITORAGGIO DEL TRAFFICO 8
- ATTACCHI DA CLIENT A CLIENT 9
- ATTACCHI BRUTE FORCE VS. ACCESS POINT 9
- ATTACCHI CRITTOGRAFICI 10
- ERRATA CONFIGURAZIONE 10

SECURITY PROBE 10

Analisi non invasiva 11
Analisi invasiva 11
Attacco 12
Consolidamento 12

4.DOCUMENTAZIONE UTENTE **13**

PIANO DI INTERVENTO **13**

ATTIVITÀ (TIPOLOGIE) 13
DOCUMENTI NECESSARI 14

RESPONSABILITÀ **14**

DOCUMENTAZIONE UTENTE 14
PIANO DI MANUTENZIONE 14

OFFERTA ECONOMICA **15**

TOTALE A VOI RISERVATO 15

CONDIZIONI GENERALI DI OFFERTA **15**

STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	11 Luglio 2008	Emissione
1.1	31 Luglio 2008	Revisione

1. RICHIESTA DEL CLIENTE

UBI SISTEMI E SERVIZI richiede di formulare una proposta, con relativa offerta economica, relativa a:

1. Interventi di WIRELESS DISCOVERY sulla propria rete, nelle sedi di Brescia e di Bergamo e VULNERABILITY ASSESSMENT WIRELESS.
2. Intervento di verifica vulnerabilità degli accessi da remoto tramite VPN
3. Intervento di verifica della V/LAN interna fornitori.
4. Intervento di verifica vulnerabilità RAS

In altre parole, si richiede una consulenza di security assessment che verifichi, secondo una logica indipendente e supra-partes, l'*effettiva* sicurezza relativa agli ambiti sopra elencati.

2. SOLUZIONE PROPOSTA

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

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

Fase A - Approccio Black Box

- Network discovery (SSID, IP, Domains)
- Access point mapping
- Analisi client misconfiguration (rogue access point)

Fase B - Documentazione

- Executive Summary
- Livello di sicurezza riscontrato e potenziali impatti sul business
- Considerazioni generali
- Descrizione attivita' svolte
- Conclusioni

2. Accessi da remoto VPN.

Fase A - Approccio Black-Box

- Analisi configurazione Server VPN

Fase B – Approccio White-Box

- Verifica raggiungibilità network e servizi con utenze fornite
- Raccolta eventuali evidenze

Fase C - Documentazione

- Executive Summary
- Livello di sicurezza riscontrato e potenziali impatti sul business
- Considerazioni generali
- Descrizione attivita' svolte
- Conclusioni

3. Verifica V/LAN interna fornitori

Fase A – Approccio Black-Box

- Verifica raggiungibilità network e servizi da interno
- Verifica presenza eventuali vulnerabilità in network e servizi raggiunti
- Raccolta eventuali evidenze

Fase C - Documentazione

- Executive Summary
- Livello di sicurezza riscontrato e potenziali impatti sul business
- Considerazioni generali
- Descrizione attivita' svolte
- Conclusioni

4. Verifica RAS

Fase A – Approccio White-Box

- Verifica raggiungibilità network e servizi (nr. verde)
- Raccolta eventuali evidenze

Fase B - Documentazione

- Executive Summary
- Livello di sicurezza riscontrato e potenziali impatti sul business
- Considerazioni generali
- Descrizione attivita' svolte
- Conclusioni

3. METODOLOGIA DELLA SOLUZIONE PROPOSTA

• Premessa

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.

• 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:

1. attacchi di inserimento
2. intercettazione e monitoraggio non autorizzato del traffico
3. jamming
4. attacchi da client a client
5. attacchi brute force all'access point
6. attacchi crittografici
7. 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:

- 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.
- 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.

- **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:

1. passivo, basato su analisi statistica del traffico
2. attivo, con iniezione di nuovo traffico da una stazione non autorizzata, basato sull'analisi del testo in chiaro passante
3. attivo, basato sulla compromissione dell'access point
4. 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.

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 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

[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.**

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.

4. DOCUMENTAZIONE UTENTE

Oltre alla documentazione sopra indicata, sarà 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.

PIANO DI INTERVENTO

Attività (tipologie)

Attività
• Attività di Discovery Wireless e Vulnerability Assessment Wireless • Attività di Vulnerability Assessment VPN + RAS • Attività di Vulnerability Assessment V/LAN interna fornitori

Documenti necessari

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

- Allegato A: Accordo Legale (Liberatoria)
- 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.

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 €
Service	**Discovery WIRELESS** (3 sites) - Frequenze standard (Attività presso vs. Sedi)	4.000
Service	**Opzione con analisi di spettro-rilevamento segnali elettromagnetici** (Attività presso vs. Sedi)	2.500
Ethical Hacking	**Vulnerability Assessment WIRELESS** (Attività presso vs. Sedi)	6.000
	Totale	**12.500**
Ethical Hacking	**Vulnerability Assessment VPN - RAS** ➢ 3 profili VPN a campione ➢ 1 profilo RAS (Attività da esterno)	7.500
Ethical Hacking	**Vulnerability Assessment V/LAN INTERNA FORNITORI** Approccio black-box (Attività presso vs. Sedi)	4.500
	Totale	**12.000**

- L'offerta è da intendersi modulare, i moduli di servizi sono attivabili singolarmente.
- 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% alla consegna report
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.