]HackingTeam[

Milano, 25 Giugno 2004

Spett.le
ISIDE
Via Rivoltana, 95
20090 Pioltello (MI)

Offerta n. 20040517.m06a

Alla c. att.ne : Dr. Alessandro Colombo

Oggetto: Offerta per servizi di Vulnerability Assessment

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

Marco Bettini
Key Account Manager

Offerta
Servizi di Vulnerability Assessment per l'ambiente open di Iside

SOMMARIO

1. STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	17 maggio 2004	Emissione
1.1	25 Giugno 2004	Aggiornamento output

2. RICHIESTA DEL CLIENTE

Iside richiede di formulare una proposta tecnico/economica relativa a servizi di Vulnerability Assessment che interessi i sistemi, i dati e le applicazioni presenti sugli ambienti open della rete interna.

In altre parole, si richiede una consulenza di security assessment che verifichi, secondo una logica indipendente e supra partes, l'*effettiva* sicurezza della rete interna, ne identifichi eventuali vulnerabilità e definisca un piano di intervento organizzativo e tecnologico che mitighi i rischi connessi.

Il dimensionamento dell'ambiente e' il seguente:

- Circa 50 server (windows o Linux)
- rete interna: circa 300 utenti + 15000 utenti potenziali delle banche clienti
- applicazioni varie (servizi web, applicazioni custom, ecc)

Si specifica inoltre che i seguenti punti saranno compresi nei risultati della consulenza in oggetto:

- Documento tecnico che riporti le vulnerabilità individuate e i passi necessari per eliminarle suggerendo le corrette policy e un piano di intervento con priorità ed impegni
- Documento di presentazione per il management in forma di *slides*.

3. METODOLOGIA PROPOSTA

Hacking Team ha adottato una metodologia di "Vulnerability Assessment" che prevede tre distinte fasi, schematizzate in Figura 1: **Analisi Iniziale, Assessment e Analisi Conclusiva**.

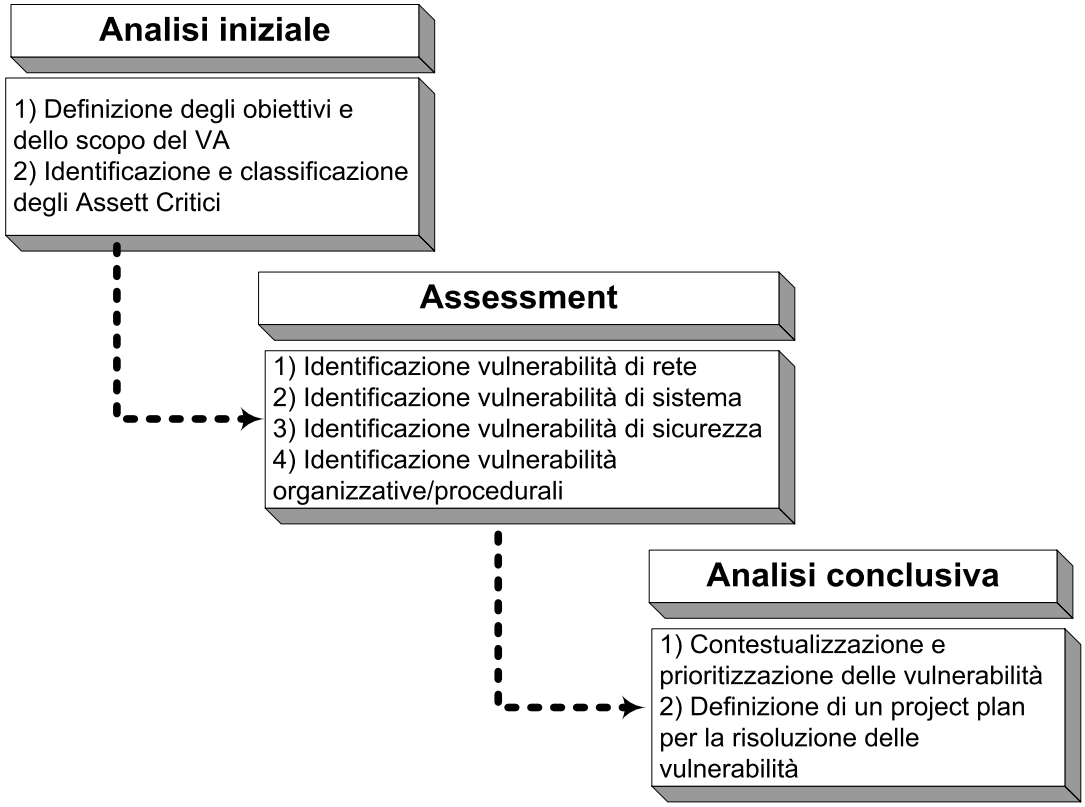

Figura 1 - Fasi di un Vulnerability Assessment

3.1. Analisi Iniziale

L'analisi iniziale è la prima fase che caratterizza un VA e consiste nel definire con precisione gli obiettivi di tale attività. Come per ogni servizio deve essere chiaro sia al committente, sia al mandatario, quali sono i risultati attesi dalla prestazione fornita. A tale scopo è importante definire e pianificare con precisione diversi aspetti:

- **L'oggetto del VA**: è necessario identificare i confini entro cui condurre l'attività in termini di sistemi informativi coinvolti.
- **Il contesto operativo**: è necessario definire la modalità e i tempi secondo cui sarà condotta l'attività sia in termini di strumenti, sia in termini di risorse coinvolte da entrambi le parti.
- **Il livello di accuratezza**: è necessario stabilire il dettaglio che si intende raggiungere con il VA al fine di pianificare correttamente le attività successive.
- **Deliverable**: è necessario definire a priori il modello e la tipologia di documentazione che il VA produrrà al fine di soddisfare le esigenze della parte committente.

Sulla base di questa analisi iniziale saranno pianificate le varie attività che caratterizzeranno le due fasi successive: assessment e analisi conclusiva. E' importante sottolineare che per valutare correttamente l'importanza delle vulnerabilità riscontrate durante la fase di assessment, i soli aspetti tecnici non sono sufficienti. Questo perché la vulnerabilità deve essere ponderata sulla base della criticità degli asset coinvolti.

L'importanza di identificare gli asset critici è ancora più evidente nella definizione del piano di risoluzione, dove la priorità e la modalità degl'interventi deve essere relazionata al valore dell'asset stesso.

Output prodotti

Gli output prodotti dalla fase iniziale saranno:

- Il project plan di tutte le attività che caratterizzeranno l'assessment (risorse coinvolte, tempi e modalità d'intervento).
- Una lista della documentazione che verrà prodotta, in termini di contenuti e tipologia.

3.2. Assessment

La parte di assessment ha lo scopo di identificare tutte le vulnerabilità che affliggono il sistema informativo. Allo scopo di classificare con precisione le diverse vulnerabilità, Hacking Team ha adottato una metodologia che definisce quattro differenti livelli:

- **Livello di rete**: in questa categoria sono inserite tutte le vulnerabilità che possono condizionare la disponibilità della rete e compromettere l'integrità e/o la riservatezza delle comunicazioni. Per identificare con precisione le lacune presenti nell'infrastruttura di rete è necessario effettuare uno studio approfondito, volto a individuarne le caratteristiche fondamentali:
  - Topologia della rete: in base alle esigenze del cliente e agli obiettivi dell'assessment verrà prodotto uno schema dell'architettura di rete a diversi livelli di dettaglio. Sulla base dei diversi schemi verranno poi identificati eventuali Point of Failure, evidenziati i punti di accesso verso reti esterne, analizzata la suddivisione logica e fisica della rete inclusa la definizione di VLAN.
  - Dispositivi: per comprendere il livello di sicurezza di una rete è necessario analizzarne i dispositivi che la costituiscono, siano essi attivi o passivi: router, switch, hub, bilanciatori di carico, etc… Per ognuna di queste componenti saranno effettuati dei controlli volti a identificare lacune dovute a errate configurazioni o eventualmente a versioni di software affette da bug.
  - Protocolli: è importante sapere quali sono i protocolli utilizzati all'interno della propria rete per poter evidenziare le lacune che li caratterizzano. Oltre ai protocolli di comunicazione è importante conoscere quali sono i protocolli di routing utilizzati.

- **Livello di sistema**: in questa categoria rientrano eventuali lacune nella configurazione del sistema operativo o delle applicazioni, vulnerabilità note dei software non aggiornati e più in generale tutti quei problemi strettamente legati ai server, alle

workstation, alle stampanti, etc…Durante il processo di analisi dei sistemi saranno presi in considerazioni diversi aspetti:

- Vulnerabilità legate a particolari versioni di software e applicazioni non opportunamente aggiornate. Questi tipi di bug sono solitamente identificati in modo automatico da strumenti di vulnerability scanning o comunque frutto di un processo di ricerca sulla base dell'ambiente oggetto del VA.
- Vulnerabilità legate a configurazioni errate che lasciano spazio ad accessi non autorizzati, comportamenti anomali (Denial of Service) o più semplicemente non hanno subito un processo di hardening. Questo processo richiede che il cliente fornisca in alcuni casi la configurazione di determinati applicativi e/o sistemi operativi, al fine di poterne valutare il livello di sicurezza (Esempio: lunghezza minima delle password, abilitazione del sistema di logging, etc…)
- La distinzione tra un sistema server e un sistema client serve a definire il livello di dettaglio che si vuole raggiungere nell'analisi delle vulnerabilità, un server sarà sicuramente più critico di un client. Per ogni sistema, con particolare attenzione per i server e il rispettivo ruolo (Web server, MAIL server, etc…), verrà prodotta una lista dei servizi attivi al fine di identificare i possibili punti di accesso in termini di applicazioni presenti.

- **Livello delle soluzioni di sicurezza**: a questa categoria appartengono le vulnerabilità dell'infrastruttura di sicurezza implementata: firewall, antivirus, intrusion detection system, etc… La competenza specifica di Hacking Team nel settore della security, consente di raggiungere un livello di analisi di dettaglio delle varie soluzioni di sicurezza adottate:
  - Sistemi firewall: per i sistemi firewall verranno analizzate le policy configurate per evidenziare eventuali lacune, la configurazione in HA, il sistema d'amministrazione e l'eventuale sistema di logging.
  - Sistemi IDS: diversi sono gli aspetti critici di un sistema di Intrusion Detection:
    - La collazione degli agenti, siano essi network sensor o host sensor.
    - Il tuning che consente di eliminare il "rumore di fondo" che affligge le soluzioni di IDS
    - Il sistema di aggiornamento delle segnature

- Sistemi Antivirus: l'adozione di diverse soluzioni di antivirus, una installata sulle singole postazioni e una a livello di gateway di posta, consente di avere una copertura complessiva.
- Virtual Private Network (VPN): la validità di una soluzione VPN è frutto dei diversi parametri di configurazioni che garantiscono al sistema differenti garanzie di sicurezza: shared secret, certificati X509, VPN baste su protocollo SSL etc…

- **Livello organizzativo/procedurale**: di questa categoria fanno parte le vulnerabilità legate agli aspetti organizzativi/procedurali in termini di politiche e strategie di backup, disaster recovery, hardening dei sistemi, password management, patching, authentication, authorization, accounting (AAA) e auditing. Spesso non è presente una politica di sicurezza esplicita e documentata. Si tratta certamente di una notevole carenza, anche perché può indicare che i meccanismi di sicurezza sono stati progettati in modo poco rigoroso e quindi possono presentare delle gravi carenze. Anche quando è presente una politica di sicurezza ufficiale tuttavia, spesso la pratica si discosta notevolmente, sia perché la politica ufficiale può essere troppo rigida (in questi casi si hanno dei tipici comportamenti di disobbedienza funzionale, in cui l'utenza della rete non rispetta la politica per poter svolgere le proprie attività in tempi ragionevoli), sia perché la mancanza di controlli sul rispetto effettivo della politica portano a comportamenti trascurati, sia perché la politica può essere stata progettata "a tavolino", non tenendo conto di molti casi reali che vengono poi gestiti con eccezioni. Anche quando la politica è presente e applicabile tuttavia, è facile trovare discrepanze notevoli fra quanto rilevato in termini di risorse critiche e minacce rilevanti, e quanto disposto dalla politica di sicurezza. In alcuni casi è possibile ad esempio che risorse estremamente critiche siano accessibili con meccanismi di sicurezza debolissimi, mentre per altre risorse, meno critiche, siano richeste procedure complesse e meccanismi di autenticazione rigorosissimi. Questi casi sono spesso dovuti a un'errata valutazione di quali siano le minacce effettivamente presenti su Internet e quale sia la loro probabilità. È allora necessario innanzitutto mettere in evidenza queste contraddizioni per avere un'indicazione chiara della reale politica dell'azienda.

Per l'identificazione delle tipologie di vulnerabilità nei diversi livelli indicati, Hacking Team ha sviluppato al suo interno tutte le competenze specifiche in ambito di sicurezza, al fine di avere una visibilità completa del panorama informativo in termini di:

- Strumenti a supporto di attività di VA: vulnerability scanner, port scanner, CGI scanner, application scanner, etc…
- Programmazione e hacking: il valore aggiunto al semplice utilizzo di strumenti standard di VA è dato dalla capacità di sviluppare propri sistemi di VA.
- Sistemi di sicurezza: per individuare una lacuna in un sistema di sicurezza, come ad esempio firewall, proxy-server, ids e antivirus, è importante conoscerne a priori il funzionamento. Tale competenza risulta particolarmente utile in fase di definizione delle contromisure e quindi nella proposta di un security project plan.

L'attività di assessment che caratterizza un VA può essere suddivisa in due macrocategorie:

- **Penetration Test Perimetrale o probe**

Un penetration test perimetrale, consiste in una verifica della sicurezza implementata sul sistema di difesa perimetrale per mezzo di attacchi simulati. Questa tipologia di servizio viene normalmente svolta senza avere informazioni fornite dalla parte committente, nell'ottica di emulare al 100% il comportamento di un vero hacker.

- **Vulnerability Assessment Interno**

Un VA interno è realizzato attraverso attacchi simulati, che a differenza dal penetration test sono effettuati dall'interno della infrastruttura informativa aziendale. Il VA interno prevede anche una fase di analisi generale dell'infrastruttura informativa e degli aspetti organizzativo/procedurali, nell'ottica di individuare lacune non esclusivamente tecniche, per poter suggerire contromisure adatte a proteggere gli asset critici per il business aziendale.

Attività di un probe

L'offerta di Hacking Team, sia per attività legate a un penetration test perimetrale, sia a un vulnerability assessment interno, seppur con qualche differenza legata alla conoscenza di

informazioni eventualmente fornite dalla parte committente, segue uno schema logico che prevede due fasi: la prima “non invasiva” e una seconda “invasiva”.
La fase non invasiva può essere suddivisa in due ulteriori stadi:

- *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 alla rete interna. Gli strumenti utilizzati sono: tecnologie di sniffing, traffic interception, DHCP discovery, IP discovery, interrogazione DNS, interrogazione WINS.
- *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” (IP discovery), quali servizi siano “attivi” (TCP/UDP port scan) e, infine, quali sistemi operativi “posseggano”. Gli strumenti utilizzati sono: interrogazioni ICMP (hping), scansione delle porte TCP e UDP (nmap, rascan), fingerprint dello stack (nmap, ettercap).

La fase invasiva può essere suddivisa in cinque ulteriori stadi:

- *ENUMERATION*: 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.
- *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 overflow, attacchi data driven, ecc.) o del sistema operativo stesso.

- *SCALATING PRIVILEGES*: 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*: 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.
- *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.

Input richiesti al committente

Al fine d'individuare con precisione le vulnerabilità presenti nel sistema informativo è importante che il committente fornisca, dove possibile e a meno di eventuali richieste legate allo specifico servizio commissionato[1], le seguenti informazioni:

- Schemi logico/fisici dell'infrastruttura informatica
- Lista dei sistemi su cui effettuare l'attività di VA
- Procedure e policy di sicurezza: backup, disaster recovery, AAA, password management, policy generiche, procedure di hardening, politiche di auditing, etc…

[1] Ad esempio in caso di Penetration Test perimetrali o comunque di attività che si intende svolgere senza fornire documentazione sull'infrastruttura informatica, ottenendo così una simulazione realistica di un attacco hacker.

Output prodotti

Gli output prodotti dalla fase di assessment saranno:

- Log di evidenza dell'attività svolta: strumenti di VA automatici, tool proprietari e azioni svolte dal personale tecnico (password ottenute, dati intercettati, etc…).
- Documentazione relativa all'infrastruttura del sistema informatico: verrà prodotto uno schema logico/fisico dell'infrastruttura IT al fine di evidenziare le lacune riscontrare.

3.3. Analisi conclusiva

L'analisi conclusiva, come si evince dal termine stesso, ha lo scopo di concludere il VA, fornendo la documentazione contenente i log di evidenza dell'attività svolta, i report delle varie tipologie di vulnerabilità riscontrate e il piano d'intervento consigliato.

La parte di documentazione relativa ai report delle vulnerabilità sarà strutturata secondo la classificazione descritta precedentemente e pesata sulla base delle criticità definite durante l'analisi iniziale. La gravità di una vulnerabilità sarà quindi frutto sia del livello d'importanza in termini tecnici (pericolosità[2]), sia in termini di business aziendale (criticità[3]).

Il piano d'intervento sarà, in modo analogo alla classificazione delle vulnerabilità, redatto tenendo in considerazione la gravità delle lacune riscontrate. Nel piano d'intervento saranno descritte in dettaglio le tipologie di risoluzione delle problematiche:

- **Workaround:** dove la vulnerabilità non e' completamente eliminabile saranno indicate le operazioni necessarie a mitigare il rischio.
- **Patching/Riconfigurazione:** dove la vulnerabilità è frutto di versioni di sw non aggiornate o semplicemente configurate erroneamente saranno indicate le operazioni per porre rimedio al problema.
- **Sviluppi futuri:** per vulnerabilità legate ad aspetti procedurali/organizzativi e a lacune infrastrutturali sarà consigliata l'adozione di opportune soluzioni e/o alternative all'attuale struttura informativa. Ad esempio potrebbe essere consigliata l'adozione di

[2] Con pericolosità s'intende quanto la vulnerabilità in questione comporti la possibilità di compromissione dei parametri di disponibilità, riservatezza e integrità dell'asset. ES: un denial of service è sicuramente meno pericolo che un escalation a diritti di amministrazione del sistema.

[3] Con criticità s'intende quanto la vulnerabilità in questione possa avere un impatto sul business aziendale: ES: un exploit remoto sarà più grave se legato a un server dove è presente il database dei miei clienti, rispetto al pc della segretaria.

un sistema di log management centralizzato per la gestione dei log dell'intera infrastruttura informativa**.**

Output prodotti

L'output prodotto dalla fase di assessment sarà il documento conclusivo, contente:

- I log di evidenza delle attività svolte.
- Le vulnerabilità riscontrate, opportunamente classificate e pesate.
- Il piano d'intervento.

In Figura 2 è mostrato il flusso logico di un Vulnerability Assessment. Sulla base della situazione attuale, dedotta dalle informazioni ottenute tramite interviste e analisi dell'infrastruttura informativa, viene prodotta una lista delle minacce esistenti. La classificazione delle minacce è frutto di un'analisi complessiva della realtà del cliente, nell'ottica di valutare non solo gli aspetti tecnici, ma soprattutto le criticità aziendali che dovrebbero essere delineate con precisione dalle security policy aziendali. In questo senso un Vulnerability Assessment può essere un ottimo punto di partenza per definire, dove non presenti, o valutare, se già presenti, le politiche di sicurezza aziendali. Il passo successivo sarà quindi identificare, correggere o implementare i diversi sistemi di sicurezza, che consentano di eliminare o ridurre le minacce rilevate dall'attività di VA.

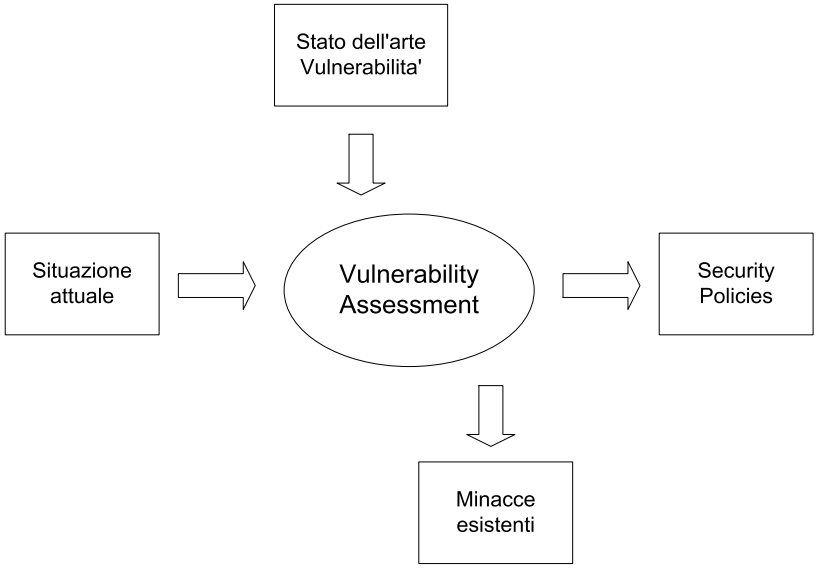

Figura 2 - Flusso logico di un Vulnerability Assessment

4. OUTPUT DI PROGETTO

Come già indicato nel capitolo 2 e nella metodologia, al termine dell'attività consegneremo:

A) Topologia e analisi della rete basate sui risultati dello studio già in vostro possesso
B) Dettagliata descrizione del metodo e degli strumenti utilizzati
C) Analisi delle vulnerabilità riscontrate:
   a) L'elenco dei sistemi/apparati accedibili in modo non autorizzato
   b) Descrizione della catena di eventi che hanno portato all'accesso della rete/sistema/applicazione
   c) Log degli eventi
   d) Eventuali esempi delle informazioni ottenute
D) Analisi delle minacce sulla base delle vulnerabilità in relazione all'ambiente di riferimento
E) Piano di intervento in termini di priorità, impegno economico e di tempo per incrementare il livello di security:
   a) Azioni di fixing e possibili miglioramenti a livello sistemistico e architetturale
   b) Studio dello scostamento delle policy esistenti rispetto a best practices applicabili all'ambiente di riferimento e alle criticità riscontrate

5. PIANIFICAZIONE PROGETTO

Nell'allegato indichiamo una pianificazione di massima delle attività.
L'indicazione dei tempi di progetto è considerata in elapsed.

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'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	Giornate Senior	Giornate Junior
Vulnerability Assessment	**A corpo**	**A corpo**

7.2. Documentazione Utente

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

Il materiale prodotto sarà fornito su supporto cartaceo e/o supporto ottico.

7.3. Totali

Descrizione	Costo a corpo
Vulnerability Assessment	**€ 25.000,00 (venticinquemilaeuro)**

Le attività di intervista e analisi verranno svolte presso la Sede di Iside, quelle relative alla preparazione della documentazione presso la Sede di Hacking Team.

7.4. Condizioni generali

Tutte le cifre sono da considerarsi IVA esclusa
Validità offerta: 30 gg
Fatturazione: 50% all'ordine
50% alla consegna della documentazione
Pagamento: 30 gg data fattura
Coordinate Bancarie: Unicredit Banca
L.go Donegani - Milano
ABI 02008 CAB 01621 C/C 000010228244 CIN A