Gruppo Toro Assicurazioni

Assessment di sicurezza interno ed esterno di reti e servizi

- Executive Summary -

Torino

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
0.1	08 Giugno 2006	Emissione bozza relativa alla parte di ethical hacking esterno
0.2	30 Giugno 2006	Emissione bozza relativa all'intera attività di ethical hacking
1.0	07 Luglio 2006	Emissione documento finale

INFORMAZIONI		
Data di Emissione	07 Luglio 2006	
Versione	1.0	
Tipologia Documento	Executive Summary	
Numero di Protocollo	//	
Numero Pagine	14	
Numero Allegati	0	
Descrizione Allegati	1	//
	2	//
Redatto da	Marco Valleri Fabio Busatto Massimiliano Oldani	
Approvato da	Gianluca Vadruccio	

INDICE

1 Introduzione

1.1 Obiettivo del lavoro

1.1.1 Rete esterna

Obiettivo dell'attività di *ethical hacking* esterno è stato simulare le azioni di un potenziale intrusore su internet che non avesse alcuna conoscenza della rete oggetto di analisi. Tale attività è stata svolta al fine di rilevare eventuali vulnerabilità della rete o dei sistemi e di valutarne il relativo impatto in termini di perdita o cattura di dati sensibili, interruzione o manipolazione dei servizi, etc.

1.1.2 Rete interna

Obiettivo dell'attività di *ethical hacking* interno è stato simulare le azioni di un potenziale intrusore che abbia già ottenuto accesso alla rete interna del cliente, sia tramite accesso diretto (dipendenti, intrusione fisica), sia tramite un accesso indiretto ottenuto sfruttando vulnerabilità presenti e utilizzabili dalla rete esterna. Tale attività è stata svolta al fine di rilevare eventuali vulnerabilità della rete o dei sistemi di ben precisi server indicati dal cliente, in maniera da identificare i possibili attacchi che non sono effettuabili dall'esterno della rete.

1.1.3 Rete dell'Agenzia

Obiettivo dell'attività di *ethical hacking* di Agenzia è stato simulare azioni di un potenziale intrusore che abbia accesso alla rete di una generica agenzia. Lo scopo è quello di identificare quali risorse appartenenti alla rete interna del cliente sono raggiungibili tramite la rete d'Agenzia (considerata esterna alla rete interna ma privilegiata negli accessi rispetto alla rete Internet), in maniera da evidenziare l'impatto che una impropria gestione della sicurezza all'interno della rete agenziale possa avere sulla sicurezza dell'intera infrastruttura del cliente.

1.2 Vincoli e limiti del lavoro svolto

Il cliente ha esplicitamente richiesto di non portare a compimento tentativi di intrusione che avrebbero potuto compromettere la stabilità dei sistemi analizzati, ma di limitarsi a evidenziare la possibilità di eseguire tali tipi di attacco qualora potessero avere concrete possibilità di successo.

1.3 Ambito e perimetro del lavoro

1.3.1 Rete esterna

L'attività di *ethical hacking* esterno è stata svolta dai laboratori di Hacking Team.
Il Cliente ha indicato una lista di società che sarebbero dovute essere oggetto di analisi; partendo da questa lista, il personale tecnico di Hacking Team ha ricercato tutte le macchine pubbliche e i domini attribuibili alle suddette società. La lista di *target* così ottenuta è stata validata dal cliente prima di procedere alle fasi più invasive dell'attività:

- gruppotoro.net
- toroassicurazioni.it
- torotarga-assicurazioni.it
- torotarga-assicurazioni.com
- augusta.it
- nuovatirrena.it

1.3.2 Rete interna

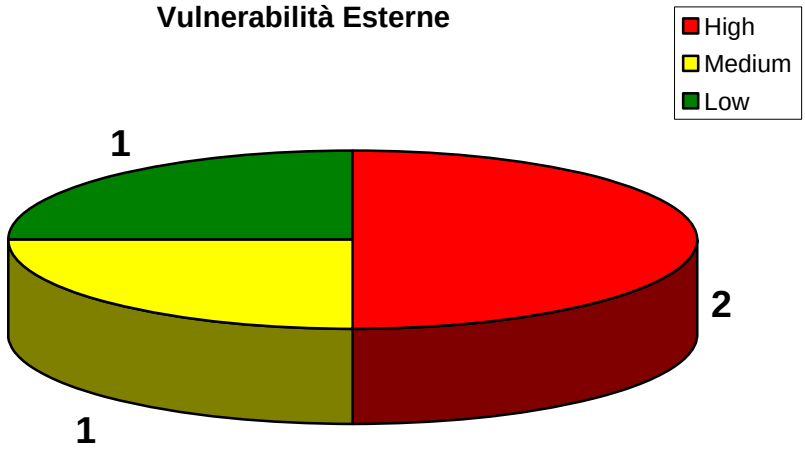
L'attività di *ethical hacking* interno è stata svolta presso i laboratori del cliente, con attrezzature proprie dei tecnici Hacking Team.
Il cliente ha indicato una lista di indirizzi di server critici appartenenti alla rete interna, i quali sono stati analizzati in maniera **indipendente dal contesto** per riscontrare le vulnerabilità presenti.

1.3.3 Rete dell'Agenzia

L'attività di *ethical hacking* interno è stata svolta presso i laboratori del cliente, predisposti al fine di emulare la configurazione di una generica agenzia per quanto riguarda la struttura della rete e l'interconnessione con la rete ed i sistemi centrali del cliente.
In questo caso non sono stati indicati obiettivi particolari, ma è stato lasciato libero campo d'azione per la ricerca di risorse sensibili raggiungibili dalla rete dell'agenzia.
L'identificazione degli indirizzi e delle reti sensibili è stata portata a termine sfruttando le conoscenze pregresse sulla topologia e sulla configurazione della rete del cliente, portate in evidenza dall'analisi della rete interna, oltre che da alcune informazioni ottenute direttamente dalle postazioni dell'agenzia.

2 Executive Summary

2.1 Parte esterna



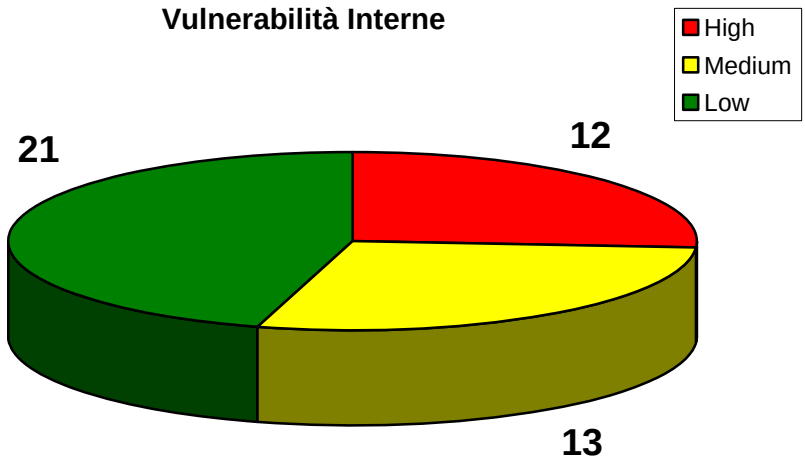
L'attività di *ethical hacking* ha evidenziato una serie di vulnerabilità sistemistiche, applicative ed architetturali che, anche se presenti in numero non elevato, hanno reso possibile l'accesso da internet alle risorse della rete interna[1] e la manipolazione dei servizi erogati da alcuni siti vetrina.
Un'analisi più approfondita ha inoltre rilevato tracce di almeno una precedente intrusione nel sistema informatico del cliente.
Va infine evidenziato come tutte le vulnerabilità elencate siano state riscontrate nei segmenti di rete di Nuova Tirrena e in quelli gestiti tramite ITS-GlobalValue. Al contrario, la sottorete assegnata a Toro Assicurazioni ha rivelato un buon livello di sicurezza.

[1] Il personale tecnico del cliente ha comunicato ad Hacking Team di aver provveduto ad eliminare il servizio vulnerabile che ha reso possibile questo tipo di intrusione.

Integrity, Confidentiality, Data Losses
➢ E' stato possibile avere accesso alla rete interna tramite una vulnerabilità su un server di perimetro. Tale rete, vista dall'esterno, ha evidenziato un grado di sicurezza non elevato. Questo rende plausibile uno scenario d'attacco in cui un intrusore esterno, senza alcuna conoscenza della rete, tramite internet, riesce ad avere accesso a dati, servizi e risorse della rete interna del Cliente. ➢ La vulnerabilità che ha permesso l'accesso alla rete interna risulta conosciuta e facile da sfruttare, e la macchina vulnerabile ha presentato evidenze di almeno una precedente intrusione. Tale intrusione ha sicuramente avuto come scopo l'utilizzo del server in questione come *IRC Bot* e *Spam Server*. Questa serie di dati rende possibile ipotizzare che lo scenario descritto nel punto precedente si sia effettivamente già verificato.
Availability
➢ E' possibile danneggiare o interrompere il servizio erogato dai siti www.toroassicurazioni.it e www.torotarga-assicurazioni.it ➢ Sempre tramite i siti del punto precedente potrebbe essere possibile leggere e modificare i dati presenti sul database alterando le informazioni pubblicate[2]

[2] In questo caso si è utilizzato il condizionale in quanto la verifica effettiva della possibilità di eseguire la modifica non è stata portata a termine, essendo in produzione l'ambiente sotto attacco. Dall'esperienza e dai sintomi che il target manifesta, la probabilità che questo possa essere realmente fattibile è decisamente alta, ma si ribadisce di non averne ad oggi la certezza.

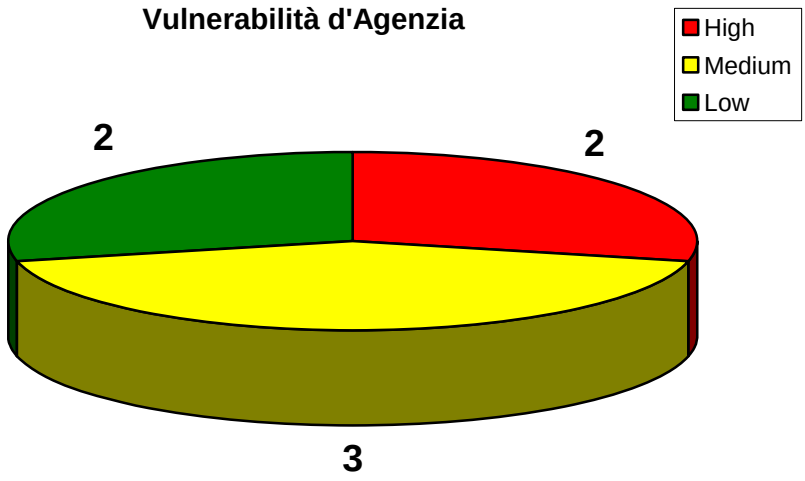
2.2 Parte interna



L'attività di *ethical hacking* ha evidenziato una serie di vulnerabilità sistemistiche presenti in numero elevato, anche se non è stato possibile compromettere le macchine in maniera semplice.
Quasi tutte le vulnerabilità sono state riscontrate su servizi di sistema che risultano non essere correttamente aggiornati, o scarsamente configurati per impedire accesso non autorizzato a dati non critici presenti sui sistemi.

Integrity, Confidentiality, Data Losses
➢ E' possibile ottenere informazioni, seppure non critiche, interrogando i servizi di informazione presenti sulle macchine e non limitati opportunamente nell'accesso
Availability
➢ Alcune vulnerabilità individuate sulle macchine della rete, anche se non facilmente sfruttabili, sono di elevata gravità e potrebbero consentire ad un eventuale attaccante di prendere il controllo remoto delle stesse. Tale controllo, in caso di successo, porta l'attaccante: o a creare dei Denial-of-service (DOS) in grado di interrompere l'attività e l'eventuale erogazione dei servizi o ad ottenere il pieno possesso delle macchine attaccate con conseguente possibile lettura o furto di informazioni o a lasciare sulla macchina un punto di ingresso per azioni di spionaggio o di utilizzo futuro incontrollato ed indisturbato

2.3 Parte dell'Agenzia



L'attività di *ethical hacking* ha evidenziato una serie di vulnerabilità sistemistiche che, se sfruttate, possono portare alla compromissione parziale o totale di alcuni server della rete interna del cliente. Il problema principale riguarda il sistema di regolamentazione degli accessi della rete interna del cliente da parte della rete dell'Agenzia, implementato da un sistema di firewalling posto tra le due reti citate. Questo apparato risulta però carente nella sicurezza, ed è quindi possibile accedere dalla rete dell'Agenzia a livello amministrativo, avendo quindi di fatto la possibilità di alterare tutto il sistema logico di protezione implementato, e rendendo di fatto quasi nullo il controllo sugli accessi. L'impatto è quindi quello di ottenere un accesso alla rete interna di tipo locale, invece di quello previsto che, sebbene sia privilegiato rispetto all'accesso dalla rete esterna, dovrebbe comunque essere più ristretto.

Le vulnerabilità elencate sono state riscontrate sulle reti 10.36.0.0 – 10.36.255.255 e sulla rete 62.123.148.0 – 62.123.148.127.

L'accesso reciproco tra le diverse agenzie ha rivelato invece un buon livello di sicurezza.

Integrity, Confidentiality, Data Losses
➢ Alcune vulnerabilità presenti sui server possono essere sfruttate per accedere a informazioni confidenziali ➢ Modificando le configurazioni del firewall a cui si è avuto accesso tramite credenziali di default è possibile alterare il normale comportamento della rete riuscendo così a raggiungere segmenti della rete interna protetti e ad intercettare il traffico di rete
Availability
➢ Alcune vulnerabilità individuate sulle macchine della rete, anche se non facilmente sfruttabili, sono di elevata gravità e potrebbero consentire ad un eventuale attaccante di prendere il

controllo remoto delle stesse. Tale controllo, in caso di successo, porta l'attaccante:
  - a creare dei Denial-of-service (DOS) in grado di interrompere l'attività e l'eventuale erogazione dei servizi
  - ad ottenere il pieno possesso delle macchine attaccate con conseguente possibile lettura o furto di informazioni
  - a lasciare sulla macchina un punto di ingresso per azioni di spionaggio o di utilizzo futuro incontrollato ed indisturbato
- Tramite l'accesso al firewall è possibile impedire il normale flusso di dati dalla rete del cliente verso la rete dell'Agenzia, impendendo il normale funzionamento del sistema di sincronizzazione delle informazioni presenti negli archivi locali delle agenzie

3 Piano dei lavori

3.1 Strategia di Fixing [3]

Step	Actions	Coverage
1	Eliminazione o aggiornamento del servizio vulnerabile *Horde* da 194.247.182.71. Questa attività risulta già essere stata portata a compimento dal personale tecnico del Cliente.	H1
2	Riscrittura del codice ASP di interfacciamento al *back-end* SQL per i siti 151.92.154.8, 151.92.154.9 e 151.92.154.74. Per minimizzare l'impatto della vulnerabilità nella finestra di tempo necessaria al completamento di questa attività (e per essere protetti anche da futuri upgrade o modifiche applicative), è consigliabile l'inserimento preventivo di un *application firewall* a presidio delle macchine interessate.	H2
3	Configurazione di una DMZ per suddividere le macchine pubbliche della *subnet* 194.247.182.64/27 dalla rete interna del Cliente (o comunque uno studio architetturale per determinare la configurazione di rete maggiormente idonea).	M1
4	Bonifica della rete interna al fine di individuare ed eliminare eventuali *backdoor* lasciate dagli intrusori potenzialmente penetrati tramite la vulnerabilità H1.	-
5	Aggiornamento dei servizi vulnerabili rilevati sulla rete interna con versioni più aggiornate rilasciate dai vendor del sistema operativo e dei prodotti utilizzati.	H3 H4 H5 M2
6	Modifica della configurazione del Cisco Firewall con credenziali di default, con appropriato piano di cambio periodico e *password management*.	H6
7	Modifica della configurazione del servizio di accesso	M3

[3] Per maggiori dettagli riguardo alle vulnerabilità elencate, fare riferimento al Report Tecnico delle attività.

	remoto VNC senza richiesta di credenziali, con appropriato piano di cambio periodico e *password management*.	
8	Controllo, sistemazione e pulizia della configurazione delle macchine.	L2 L3 L4

3.2 Security Plan

Step	Actions
1	Studio e progettazione di rete per l'introduzione di una DMZ e controllo/ottimizzazione delle regole di firewalling e di routing.
2	Adottare un sistema automatico di aggiornamento delle piattaforme e del software o, in alternativa, una procedura di aggiornamento efficace e controllata.
3	Adottare una procedura completa e controllata di installazione e blindatura degli apparati di rete e delle piattaforme server.
4	Pianificare l'inserimento di un sistema di protezione delle applicazioni sensibili erogate via web.
5	Bonificare la rete interna verificando la pulizia delle macchine e la non presenza di trojans e/o backdoors.
6	Analizzare e migliorare il controllo e la sicurezza delle connessioni verso le agenzie.

4 Attività consigliate

Il lavoro svolto è senz'altro utile ed ha evidenziato vulnerabilità critiche la cui sistemazione è necessaria per la protezione degli assets critici del cliente, ma può definirsi tutt'altro che completo.
Di seguito si consigliano alcune attività che Hacking Team potrebbe offrire al Cliente al fine di integrare il lavoro effettuato, analizzando ed approfondendo aspetti correlati che non erano coperti dalle precedenti richieste.
Ogni indicazione è indipendente, e si pone come obiettivo quello di assicurare una copertura completa della ricerca di vulnerabilità e di punti deboli dell'intero sistema.

4.1 Vulnerability assessment della rete interna nel suo complesso

Durante il presente incarico è stata testata la sicurezza di alcuni server posizionati sulla rete interna, evidenziando la presenza di vulnerbilità abbastanza comuni e simili sulle varie macchine. Nonostante quest'analisi sia stata svolta in modo esauriente e completo, non è possibile indicare quale sia il grado di sicurezza della rete interna. Questo è dovuto al fatto che un attacco all'infrastruttura può essere condotto sia sfruttando debolezze nei server critici, sia sfruttando vulnerabilità di qualsiasi macchina che con essi comunichi in qualche modo. Considerando l'attenzione sempre maggiore che le società pongono verso i server sensibili, solitamente è difficile trovare delle minacce serie su di essi; molto più facilmente si trovano situazioni in cui la macchina attaccata è, ad esempio, quella di un amministratore che gestisce le macchine o una figura dipendente che può accedere ai dati sensibili (attacco ponte). Per uno studio completo che tuteli il cliente e la sua sicurezza interna si rende necessario quindi valutare le minacce presenti nella rete nel suo complesso.
L'indicazione è quindi quella di far testare la sicurezza della rete interna, non limitatamente ad alcuni server critici ma nel suo complesso, potendo spaziare anche sulle macchine non critiche e sulle infrastrutture (switch, router) che forniscono l'interconnessione tra le macchine.

4.2 Vulnerability assessment applicativo

L'analisi applicativa consiste nello studio delle vulnerabilità delle applicazioni web, sia con credenziali che senza, in maniera da capire come la logica possa essere sovvertita per poter avere accesso ad informazioni non autorizzate.

Durante il presente lavoro non è stato approfondito l'aspetto applicativo, in quanto al di fuori delle richieste del cliente. Solo una semplice analisi superficiale ha portato comunque alla luce alcune vulnerabilità delle applicazioni (paragrafo **Errore. L'origine riferimento non è stata trovata.**).
L'indicazione è quindi quella di far testare la sicurezza delle applicazioni in maniera più mirata (application analysis, source code analysis), fornendo eventualmente credenziali di accesso per poter analizzare anche le parti non accessibili in maniera anonima.

4.3 Bonifica post-intrusione dell'ambiente

L'intrusione rilevata durante l'analisi dei sistemi dall'esterno deve essere integrata con uno studio focalizzato all'individuazione delle azioni compiute dagli attaccanti all'interno dell'infrastruttura del cliente. Il fatto che qualcuno abbia già attaccato con successo la rete è un dato certo, visto quanto trovato installato sul server di posta web (paragrafo **Errore. L'origine riferimento non è stata trovata.**); ma oltre a quanto trovato, l'attaccante in questione avrà compiuto altre azioni all'interno della rete sfruttabili poi in un secondo momento senza che nessuno se ne accorga?
Lo scopo di questa analisi è di individuare eventuali altri sistemi compromessi dagli attaccanti sfruttando il primo ingresso come ponte per accedere alla rete interna del cliente (evento da non sottovalutare vista la sua semplice fattibilità).
Questo comporta uno studio della macchina offesa, in unione con uno studio più approfondito delle possibili tracce e indizi della presenza di altre compromissioni all'interno dell'infrastruttura.