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*

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
0.1	08 Giugno 2006	Emissione bozza relativa alla parte di ethical hacking esterno
//	//	//
//	//	//

INFORMAZIONI		
Data di Emissione	08 Giugno 2006	
Versione	0.1 (BOZZA)	
Tipologia Documento	Executive Summary	
Numero di Protocollo	//	
Numero Pagine	10	
Numero Allegati	0	
Descrizione Allegati	1	//
	2	//
Redatto da	Marco Valleri	
Approvato da	Gianluca Vadruccio	

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

INDICE

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

1 Introduzione

1.1 Obiettivo del lavoro[1]

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.

1.2 Vincoli e limiti del lavoro svolto[2]

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[3]

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] Il contenuto del presente paragrafo è limitato esclusivamente alla parte di studio legata al perimetro esterno della rete. Il documento finale conterrà il restante studio: parte interna e agenziale.

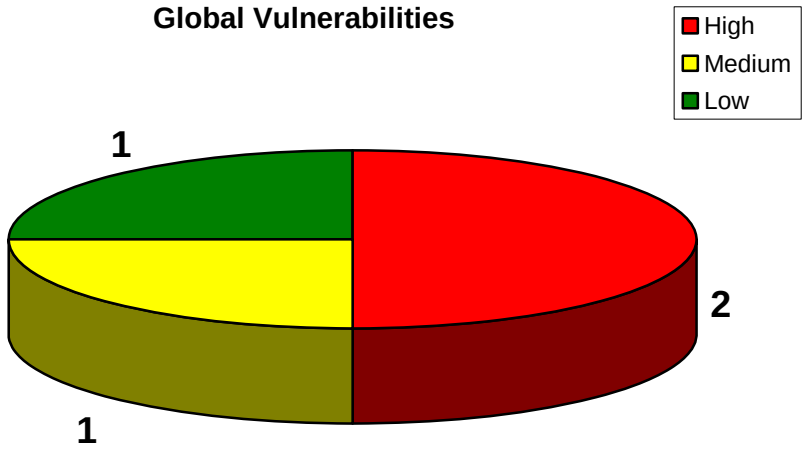
[2] Il contenuto del presente paragrafo è limitato esclusivamente alla parte di studio legata al perimetro esterno della rete. Il documento finale conterrà il restante studio: parte interna e agenziale.

[3] Il contenuto del presente paragrafo è limitato esclusivamente alla parte di studio legata al perimetro esterno della rete. Il documento finale conterrà il restante studio: parte interna e agenziale.

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

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[4] 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.

[4] 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.

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

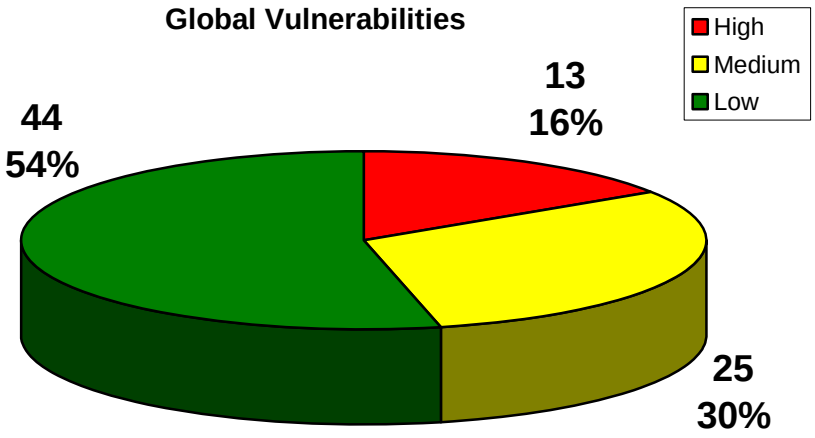
Integrity, Confidentiality, Data Losses
➢ E' stato possibile avere accesso alla rete interna tramite una vulnerabilità su un server di perimetro. Tale rete, vista dall'esterno, ha evidenziato un grado di sicurezza non elevato. Questo rende plausibile uno scenario d'attacco in cui un intrusore esterno, senza alcuna conoscenza della rete, tramite internet, riesce ad avere accesso a dati, servizi e risorse della rete interna del Cliente[5]. ➢ 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[6]

[5] L'effettivo grado di sicurezza della rete interna sarà verificato nelle successive fasi dell'attività.

[6] 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.

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

2.2 Parte interna



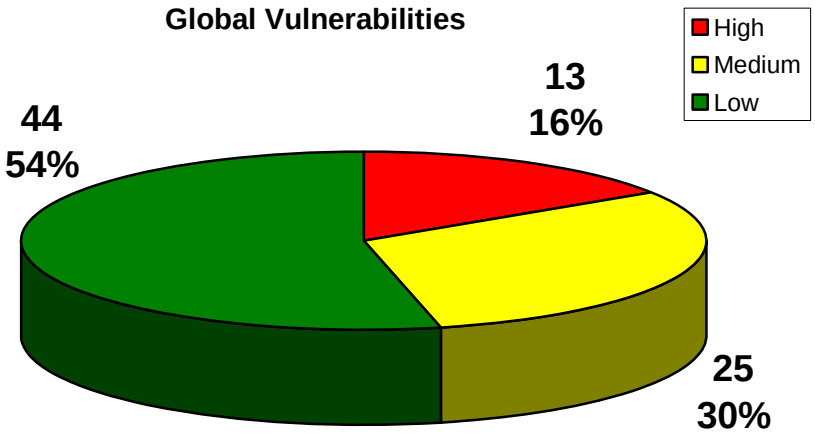
Descrizione

Integrity
➢ 1 ➢ 2 ➢ 3
Availability
➢ 1 ➢ 2 ➢ 3
Confidentiality
➢ 1 ➢ 2 ➢ 3
Data Losses
➢ 1 ➢ 2 ➢ 3

Descrizione

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

2.3 Parte agenziale



Descrizione

Integrity
➢ 1 ➢ 2 ➢ 3
Availability
➢ 1 ➢ 2 ➢ 3
Confidentiality
➢ 1 ➢ 2 ➢ 3
Data Losses
➢ 1 ➢ 2 ➢ 3

Descrizione

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

3 Security Plan[7]

Step	Actions	Coverage
1	Eliminazione 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, 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.	M1
4	Bonifica della rete interna al fine di individuare ed eliminare eventuali *backdoor* lasciate dagli intrusori potenzialmente penetrati tramite la vulnerabilità H1.	-

[7] Per maggiori dettagli riguardo alle vulnerabilità elencate, fare riferimento al Report Tecnico dell'attività.

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

4 Attività consigliate

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.