Gruppo Toro Assicurazioni

Assessment di sicurezza interno ed esterno di reti e servizi

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 dall'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	Documento di Progetto	
Numero di Protocollo	//	
Numero Pagine	54	
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.
Inoltre, il raggio d'azione dell'attacco esterno è stato completo; quello relativo all'attaco interno si è limitato ad una lista di server considerati critici dal cliente.

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 Principi generali

I principi metodologici che seguono sono stati impiegati nella valutazione dei livelli di sicurezza e nella formulazione delle soluzioni tecniche proposte.

2.1 Principio del privilegio minimo

"Tutto quello che non è strettamente necessario deve essere eliminato"

E' il principio più importante da seguire in materia di sicurezza. Il principio del privilegio minimo "minimum privilege" afferma che ogni *soggetto* all'interno di un sistema informatico (utenti, processi, programmi) deve essere in grado di accedere solamente agli *oggetti* del sistema (dati, accessi, flussi di dati, operazioni sui dati) di cui ha strettamente bisogno per le proprie funzioni. Il principio del privilegio minimo è fondamentale, perchè limita l'esposizione degli oggetti ad eventuali attacchi e, al tempo stesso, limita i danni subiti dall'intero sistema nel caso che un "attacco" abbia successo.

2.2 Principio della ridondanza

"Ogni meccanismo di sicurezza si può inceppare"

La sicurezza di un sistema (o di una procedura, di una funzione, di un'applicazione) non deve dipendere da un solo meccanismo di sicurezza, per quanto esso possa sembrare robusto e infallibile. E' sempre auspicabile prevedere delle soluzioni di "backup" che possano intervenire nell'evenienza di una temporanea indisponibilità di una risorsa adibita alla protezione del sistema o in presenza di un "attacco" sferrato contro la risorsa stessa.

Per esempio, è buona norma duplicare le procedure di logging quando l'auditing delle applicazioni è security-critical per il business aziendale. Oppure, assumere che le misure di sicurezza principali per il controllo dell'integrità possano in qualche modo essere "bypassate", e impiegare dei sistemi di controllo di flusso che abbiano la funzionalità di controllare che le misure di sicurezza principali siano ben funzionanti.

A supporto di quanto è stato detto, bisogna osservare che tutte le tecnologie di security soffrono di un'obsolescenza assai più rapida rispetto agli strumenti software convenzionali.

La qualità e l'efficacia degli attacchi che possono essere effettuati contro un sistema informatico è in costante evoluzione, e per questa ragione è necessario che le misure di sicurezza rispecchino le nuove tecniche di attacco non appena queste diventano note.

Internet è un formidabile catalizzatore del processo evolutivo “nuovo attacco - nuova misura di sicurezza per rendere inefficace l’attacco - nuovo attacco in grado di neutralizzare la misura di sicurezza precedente”. È opportuno ipotizzare che anche il personale interno all’azienda possa essere in grado di procurarsi informazioni e tecnologie sufficienti a sfruttare le debolezze della infrastruttura.

2.3 Principio della globalità

“Una catena è forte quanto il suo più debole anello”

Un’infrastruttura informatica complessa è composta da numerosi elementi strettamente interconnessi.

La sicurezza dell’intera infrastruttura è il risultato della sicurezza dei singoli elementi e, soprattutto, della sinergia che i singoli elementi, una volta raggruppati, riescono a formare. Non ha senso rafforzare massicciamente la sicurezza di un solo elemento lasciandone vulnerabile un altro: in tal caso, chi compie la frode informatica sfrutterà l’insicurezza di quest’ultimo per violare la sicurezza dell’intero sistema.

Chi è intenzionato a violare la sicurezza del sistema cercherà di “passare” per la strada più breve, cioè per quella con il più conveniente rapporto costi / benefici. Spesso la via più facile per accedere illegalmente alle informazioni non è affatto tecnica.

Talvolta è preferibile, per l’hacker, acquisire le informazioni che desidera corrompendo un addetto interno piuttosto che tentando un attacco tecnico ad alta sofisticazione come la crittoanalisi di un algoritmo crittografico con cui sono protetti i dati.

2.4 Principio dell’unico punto di contatto

“E’ più facile controllare un unico punto di passaggio”

E’ buona norma concentrare le funzioni di sicurezza applicative, di rete, ecc. su di un numero esiguo di sistemi, in maniera che la sicurezza dell’intera infrastruttura dipenda da pochi punti altamente controllabili.

2.5 Principio della modularità

“E’ più facile controllare la sicurezza di piccoli oggetti”

Oggetti piccoli sono più facilmente gestibili e controllabili. Nel caso che un oggetto fallisca, la sicurezza dell’intera infrastruttura può essere preservata. Un oggetto piccolo, inoltre, ha una complessità inferiore rispetto ad un oggetto grande e integrato ed è quindi più difficile che al suo interno siano contenute debolezze applicative (“bugs”). Questo principio permette anche di

individuare con maggiore facilità le parti più critiche del sistema, dando la possibilità di interventi il più possibile mirati nell'evenienza di aggiunte, potenziamenti o aggiornamenti di ciascuna delle componenti.

2.6 Principio della ben definita politica di sicurezza

"Nel dubbio, meglio negare che permettere"

Nella progettazione di un sistema di sicurezza sono possibili due approcci:

1. Quello che non è espressamente permesso è proibito
2. Quello che non è espressamente proibito è permesso

In linea generale, il primo approccio è sempre preferibile dal punto di vista della sicurezza.

2.7 Principio della semplicità

"KISS: Keep It Simple Stupid"

La semplicità va d'accordo con la sicurezza. Ma complessità va d'accordo con la mancanza di visibilità da cui, immancabilmente, scaturisce l'insicurezza. Le componenti di un sistema di sicurezza devono essere il più semplici possibili, affinchè il sistema risulti facile da usare e da gestire. E' un errore storico quello di pensare che un sistema grande e complesso debba essere sicuro. Un sistema grande e complesso è tipicamente difficile da analizzare, fino a diventare *oscuro.*

Quello che per noi è difficile da capire può apparire cristallino agli occhi di chi vuole compiere una frode informatica. La semplicità, quindi, gioca dalla nostra parte: più un oggetto è semplice, più una procedura è comprensibile e maggiori sono le probabilità che sia sicura. E' noto dall'ingegneria del software che i programmi complessi hanno più "bugs" e tra questi è probabile che ce ne siano alcuni relativi alla sicurezza[1].

2.8 Principio di Kerchhoff

"Chi compie la frode conosce sempre tutti i dettagli implementativi"

Se la robustezza di un sistema di sicurezza è basata sul fatto che non siano pubblicamente noti gli "internals", gli algoritmi o le specifiche tecnologie usate, allora il sistema in questione è assai insicuro. E' un approccio errato credere che, al fine di aumentare la sicurezza, sia meglio mantenere la propria tecnologia di difesa segreta piuttosto che lasciare che tale tecnologia venga visionata da un grande numero di esperti. Assumere che sia un compito difficile effettuare il

[1] Alcuni studi dimostrano che, in fase di sviluppo di codice, ogni circa 200 righe viene introdotto un bug.

“reverse engineering” di un’applicazione è un grave errore, un errore che purtroppo viene commesso da molti. I migliori oggetti di sicurezza sono quelli che impiegano algoritmi e protocolli pubblici che sono stati attaccati, analizzati e corretti per anni dai migliori esperti di sicurezza. E’ storicamente noto come moltissimi prodotti definiti *proprietary* sono risultati del tutto insicuri ed inadeguati una volta che i loro internals sono stati scoperti e resi pubblicamente noti.

3 Metodologia

La metodologia di assessment utilizzata da Hacking Team si fonda su un approccio iterativo, che prevede l'esecuzione ciclica di cinque attività:

- analisi (architetturale ed implementativa);
- identificazione delle vulnerabilità;
- definizione degli scenari di attacco;
- esecuzione degli attacchi/validazione degli scenari;
- definizione delle contromisure.

La necessità di operare in modo iterativo nasce dal fatto che l'esecuzione di ogni attacco può accrescere il livello di conoscenza del sistema e/o il livello di privilegio di chi lo esegue, rendendo necessaria una nuova fase di analisi, sulla cui base identificare nuovi scenari di attacco.

L'assessment si conclude quando, sulla base di tutte le informazioni raccolte e dei privilegi ottenuti non si possono identificare ulteriori scenari di attacco. L'output dell'assessment è costituito dal presente documento, che descrive:

- come la metodologia è stata applicata al caso particolare in esame;
- i risultati degli attacchi effettuati;
- le contromisure da adottare per eliminare le vulnerabilità individuate.

I prossimi sottoparagrafi descrivono in maggior dettaglio le modalità di esecuzione delle singole attività previste dalla metodologia utilizzata.

3.1 Analisi

Questa fase consiste nella raccolta di informazioni relative ai sistemi oggetto del vulnerability assessment, sulla cui base definire la strategia di analisi e di attacco.

Le informazioni raccolte sono sia di carattere funzionale (scopo del sistema, tipologie di utenti, dati trattati, ecc.), sia di tipo tecnico (piattaforma HW/SW, tecnologie, servizi presenti, ecc.).

Le modalità di reperimento delle informazioni sono molteplici:

- incontri con sviluppatori e/o responsabili;
- documentazione fornita dal Cliente;
- analisi diretta del sistema.

3.1.1 Strumenti utilizzati

Nella fase di analisi ci si avvale dei seguenti tool.

- ***Scanner di rete***: sono tool che eseguono in modo automatico la ricerca dei servizi presenti sul sistema obiettivo, fornendo indicazioni su quali porte sono aperte e su quali servizi possono essere acceduti.
- ***Scanner di vulnerabilità***: sono tool più avanzati che permettono di identificare in maniera automatica la vulnerabilità dei servizi presenti che sono stati identificati tramite uno scanner di rete, basandosi sia sul confronto delle versioni riscontrate rispetto ad un database costantemente aggiornato, sia tramite attacchi attivi effettuati nel tentativo di sfruttare le vulnerabilità ipotizzate.

3.2 Identificazione delle vulnerabilità

Questa fase consiste nella ricerca di errori logico/architetturali ed implementativi che possono essere sfruttati per compromettere la sicurezza del sistema.
Le tecniche utilizzate per le due classi di errori sono differenti.

- Gli ***errori di tipo logico/architetturale*** dipendono dall'applicazione in esame; la loro identificazione deve essere fatta manualmente, da parte di figure professionali che, sulla base della propria esperienza, siano in grado di riconoscere pattern di vulnerabilità generici nella logica di una particolare applicazione. In alcuni casi, l'analisi manuale può portare ad identificare anche debolezze architetturali specifiche, non riconducibili a nessun pattern noto. In questa fase, l'utilizzo di tool automatici è limitato ai proxy HTTP, che permettono di analizzare e modificare i flussi di input/output dell'applicazione.
- Gli ***errori implementativi*** vengono identificati analizzando l'output prodotto dall'applicazione in risposta ad input costruiti in modo tale da produrre comportamenti inattesi. Utilizzando un database contenente vulnerabilità note e relative tecniche di attacco, si procede mediante applicazione sistematica di tali tecniche di attacco, analizzando poi l'output ottenuto. La ricerca di errori implementativi può essere efficacemente supportata da tool automatici, che garantiscono velocità e completezza, sia in termini di parametri di input analizzati, sia in termini di test effettuati. L'intervento umano rimane comunque necessario per l'eliminazione dei falsi positivi, cioè quelle vulnerabilità individuate dai tool automatici, che non sono effettivamente presenti nell'applicazione.

3.3 Definizione degli scenari di attacco

L'individuazione di una singola vulnerabilità non è sufficiente, nella maggior parte dei casi, per compromettere la sicurezza di un sistema. Un attacco che abbia come obiettivo l'accesso ad informazioni riservate, il furto di identità ad altri utenti, o, in generale, qualsiasi utilizzo non

consentito del sistema richiede l'elaborazione di una strategia articolata che comprende relative tecniche e sfrutta diverse vulnerabilità.

E' quindi necessario, sulla base dei risultati della fase di individuazione delle vulnerabilità, definire le strategie di attacco che possono essere utilizzate per uno specifico sistema. Questa attività deve essere svolta caso per caso in modo completamente manuale, da parte di figure professionali con competenze sia di livello architetturale/sistemistica, sia implementativo.

3.4 Esecuzione degli attacchi

Poiché il vulnerability assessment viene svolto senza avere accesso al sistema, l'effetto di un attacco può essere determinato soltanto mediante la sua effettuazione. Questa fase può richiedere l'utilizzo di programmi *ad hoc* per realizzare gli attacchi individuati nella fase precedente.

3.4.1 Strumenti utilizzati

Nella fase di analisi ci si avvale dei seguenti tool.

- ***Password crackers***: programmi che permettono di identificare la password di un determinato account tramite il tentativo reiterato di password costruite secondo una determinata logica, basandosi soprattutto su dizionari esistenti o creati *ad-hoc*.
- ***Known exploits***: spesso le vulnerabilità possono essere sfruttate utilizzando dei codici creati appositamente per ottenere l'accesso tramite il servizio vulnerabile presente sul sistema.

3.5 Definizione delle contromisure

L'attività di vulnerability assessment si conclude con la stesura di un report che descrive l'analisi svolta, gli scenari di attacco individuati, i tentativi di attacco eseguiti ed il loro esito. Per gli attacchi che hanno avuto successo viene riportata la descrizione delle vulnerabilità che lo hanno reso possibile, gli errori logici o implementativi che ne sono la causa e gli interventi correttivi necessari per l'eliminazione del problema.

4 Analisi topologica ed architetturale

4.1 Studio rete esterna

L'attività di *network reconnaissance* ha identificato tre segmenti di rete principali che ospitano le macchine del Cliente risultate attive:

- **TORO2 [62.123.229.128 - 62.123.229.191]** – Questa rete è intestata a Toro Assicurazioni SPA e risulta protetta da un sistema di tipo IPS.
- **NUOVATIRRENA [194.247.182.64 – 194.247.182.95]** – Questa rete è intestata a Nuova Tirrena SPA e risulta protetta da un sistema di filtraggio del traffico (*firewall*).
- **ITS-NET [151.92.0.0 - 151.92.255.255]** – Questa rete risulta intestata a ITS, e solo una piccola parte degli indirizzi sono utilizzati dalle macchine del cliente.

4.2 Studio rete interna

L'attività sulla rete interna non è stata finalizzata a scoprire vulnerabilità infrastrutturali dell'intera architettura interna, quanto piuttosto si è limitata all'analisi della sicurezza e alla ricerca delle vulnerabilità di alcuni server che, per la loro posizione, risultano raggiungibili solo tramite un collegamento diretto con la rete interna, mentre non risultano raggiungibili alla stessa maniera da un collegamento Internet.

L'analisi effettuata si è quindi svolta posizionandosi presso la rete interna del Cliente e potendo così raggiungere gli indirizzi indicati dal Cliente stesso come server critici da controllare.

Tutti gli indirizzi testati appartengono alla rete interna principale del Cliente, con indirizzamento 10.36.0.0 – 10.36.255.255.

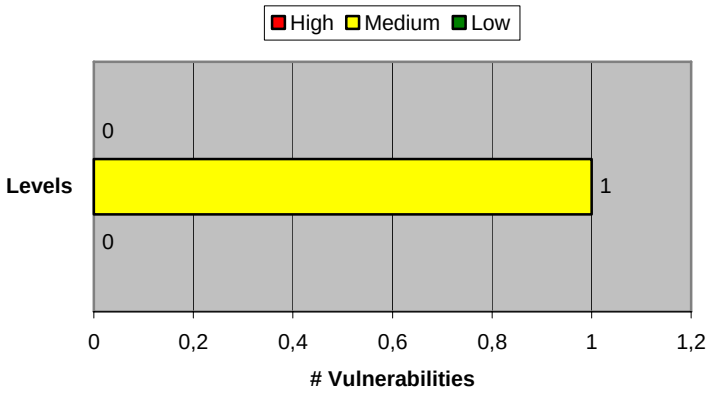
4.3 Studio rete dell'Agenzia

L'attività sulla rete dell'Agenzia è stata suddivisa in tre parti:

- analisi delle sottoreti raggiungibli dalla rete Agenziale messa a disposizione dal cliente
- analisi delle vulnerabiità delle macchine gestite direttamente dal Cliente e raggiungibili dalla postazione dell'Agenzia

L'analisi effettuata si è quindi svolta da una postazione presso il Cliente cercando di raggiungere le suddette reti: 62.123.148.0 - 62.123.148.127 e 10.36.0.0 – 10.36.255.255.

4.4 Vulnerabilità architetturali



#n	Level	Description	Threat	Fix
M1	Medium	Almeno una delle macchine ospitate dalla sottorete pubblica 194.247.182.64/27 è risultata collegata direttamente anche alla rete interna del Cliente.	Una macchina del perimetro, se compromessa, può essere utilizzata per effettuare attacchi alla rete interna (generalmente meno protetta e filtrata).	Creazione di una DMZ attraverso l'inserimento di un sistema di filtraggio del traffico fra i server del perimetro e la rete interna, o corretta configurazione delle regole di *filtering* qualora un dispositivo di tal tipo sia già presente.

5 Ethical Hacking esterno

L'attività di *ethical hacking esterno,* svolta da Hacking Team, ha avuto come oggetto di analisi le macchine (server ed apparati) facenti parte del perimetro di rete del Cliente e, pertanto, raggiungibili tramite la rete internet. Questa fase dell'attività è stata quindi svolta dagli uffici di Hacking Team.

Il Cliente non ha indicato le classi di indirizzamento, o i domini da analizzare, ma ha fornito unicamente i nomi delle società che sarebbero dovute rientrare nell'attività di *ethical hacking*. La prima parte dell'attività ha quindi avuto come obiettivo l'individuazione dei domini e delle sottoreti associabili a tali società; tale individuazione è avvenuta tramite interrogazioni a database pubblici (motori di ricerca, DNS, whois, etc.).

Prima di procedere con le fasi più invasive dell'analisi, la lista dei domini e delle macchine individuate è stata validata dal Cliente.

5.1 Rete [62.123.229.128 - 62.123.229.191]

5.1.1 Descrizione

La sottorete in questione è registrata presso il RIPE come TORO2-IT. La registrazione è a carico di TORO ASSICURAZIONI SPA e il contatto di riferimento risulta essere f.bongiovanni@toroassicurazioni.it. Le macchine ospitate in questa sottorete sono risultate, per dichiarazione del Cliente, protette da un sistema IPS. Questo sistema ha reso più complesso e meno affidabile il processo di *scanning* automatico dei sistemi: non è stato infatti possibile determinare se l'assenza di vulnerabilità rilevate fosse riconducibile ad una perfetta configurazione dei sistemi o alla presenza di un apparato di filtraggio del traffico.

5.1.2 62.123.229.134

Generali Info		
OS fingerprint	-	
Open TCP services	Number	Service
	80	HTTP
	443	HTTPS

- I servizi WEB erogati dalla macchina risultano essere mediati da WebSEAL 5.1.0.0, che funge da *reverse-proxy*.
- Pur non essendo stata oggetto di uno specifico test applicativo, la *form* di *login* presentata dal servizio non ha evidenziato vulnerabilità macroscopiche.

5.1.3 62.123.229.134

Generali Info		
OS fingerprint	-	
Open TCP services	Number	Service
	80	HTTP
	443	HTTPS

- I servizi WEB erogati dalla macchina risultano essere mediati da WebSEAL 5.1.0.0, che funge da *reverse-proxy*.
- Pur non essendo stata oggetto di uno specifico test applicativo, la *form* di *login* presentata dal servizio non ha evidenziato vulnerabilità macroscopiche.
- Va rilevato che se viene fornita come password la stringa "*passwd*", il sistema non ritorna il consueto messaggio di login fallita, ma chiude inaspettatamente la connessione.

5.1.4 62.123.229.138

Generali Info		
OS fingerprint	Windows 2003	
Open TCP services	Number	Service
	80	HTTP

- Il servizio WEB è erogato tramite IIS 6.0
- La home page del servizio non è direttamente raggiungibile tramite browser (il server restituisce un errore HTTP 403/Forbidden).

5.1.5 62.123.229.172

Generali Info		
OS fingerprint	Windows 2000-2003	
Open TCP services	Number	Service
	80	HTTP
	443	HTTPS

- Il servizio WEB è erogato tramite IIS 5.0

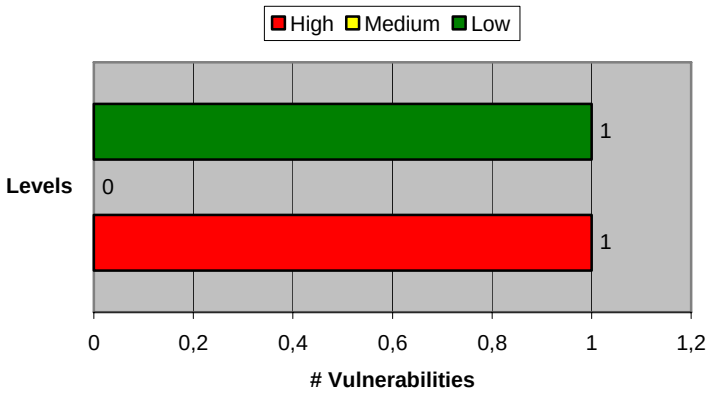
5.2 Rete [194.247.182.64 - 194.247.182.95]

5.2.1 Descrizione

La sottorete in questione è registrata presso il RIPE come NUOVATIRRENA. La registrazione è a carico di Nuova Tirrena SpA.

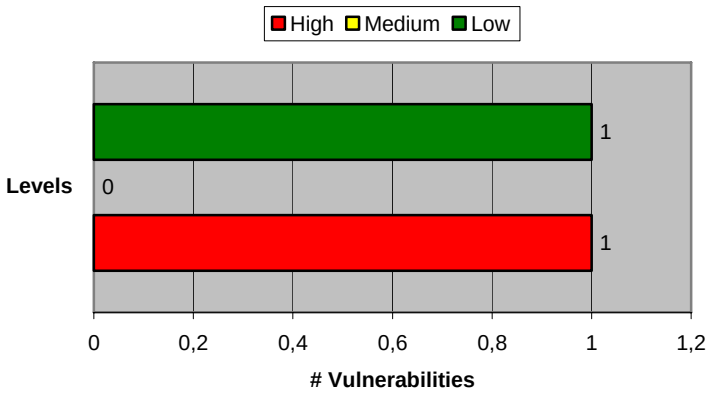
Almeno una delle macchine ospitate da questa sottorete è risultata collegata direttamente anche alla rete interna del Cliente (o quantomeno non è stato individuato nessun dispositivo di filtraggio del traffico tra essa e la rete interna). Questo ha permesso, in seguito alla compromissione della macchina, di avere accesso ai sistemi e ai servizi della rete interna (vedere paragrafi 4.4 e 6).

5.2.2 Summary



Main Vulnerabilities		
Name	Description	IP
Horde Help Viewer Remote PHP Code Execution Vulnerability (BID 17292)	E' possibile utilizzare un bug nel *parsing* dell'input del servizio Horde per installare ed eseguire software sulla macchina.	194.247.182.71

5.2.3 194.247.182.71



Generali Info		
OS fingerprint	Linux 2.6.x	
Open TCP services	Number	Service
	22	SSH
	80	HTTP
	110	POP3

- La macchina offre servizi di posta (POP e WebMail).
- Il servizio WEB è gestito tramite un server Apache 2.2.0 con PHP4.4.0.
- Il servizio SSH è gestito tramite OpenSSH 4.0 e supporta le versioni SSHv1 e SSHv2.
- E' stato possibile installare ed eseguire da remoto programmi su questa macchina.
- E' stato possibile utilizzare questa macchina come testa di ponte per esplorazioni e attacchi della rete interna del Cliente.
- **Questa macchina è risultata già compromessa prima dell'attività di ethical hacking**. I presunti attaccanti hanno utilizzato il server come *IRC Bot* e *Spam Server.* E' possibile ipotizzare (anche se non ve ne sono evidenze), che tali attaccanti abbiano inoltre usato questa macchina come testa di ponte per esplorazioni o attacchi della rete interna (vedere paragrafi 4.4 e 7)

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
H1	High	Horde Help Viewer Remote PHP Code Execution Vulnerability (BID 17292)	E' possibile utilizzare un bug nel *parsing* dell'input del servizio Horde per installare ed eseguire software sulla macchina.	Sfruttando questa vulnerabilità è possibile installare il software necessario sulla macchina per utilizzarla come testa di ponte per attacchi verso la rete interna, oltre che per carpire i dati e le credenziali di chi utilizza il servizio di WebMail.	Tutte le informazioni necessarie alla gestione della vulnerabilità sono presenti all'URL http://www.securityfocus.com/bid/17292. Il personale tecnico ha comunque già provveduto ad eliminare il servizio incriminato.
L1	Low	Information Leaking	E' possibile ottenere informazioni sulla macchina effettuando il *browsing* di file e directory installate di default, ad esempio: • /horde/test.php?mode=phpinfo • /html/	Le informazioni ottenibili possono essere utilizzate da un attaccante per massimizzare le possibilità di successo di un'intrusione.	E' sufficiente rimuovere le componenti precedentemente elencate che non sono esplicitamente necessarie per l'erogazione del servizio.

5.2.4 194.247.182.73

Generali Info		
OS fingerprint	Windows 2003	
Open TCP services	Number	Service
	21	FTP
	80	HTTP
	443	HTTPS
	1723	PPTP

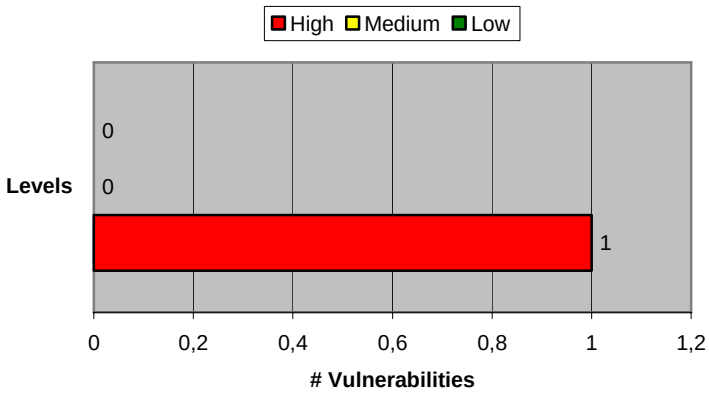
- Il servizio WEB è erogato tramite IIS 6.0.

5.3 Rete [151.92.0.0 - 151.92.255.255]

La sottorete in questione risulta essere registrata a carico di ITS-GlobalValue. Non tutti gli indirizzi facenti parte di questa *subnet* sono pertanto assegnati al Cliente. L'individuazione delle macchine che sarebbero dovute rientrare nell'attività di *ethical hacking* è stata quindi effettuata tramite delle richieste di *zone transfer* al DNS autoritativo (*ns.its.it*) per i seguenti domini:

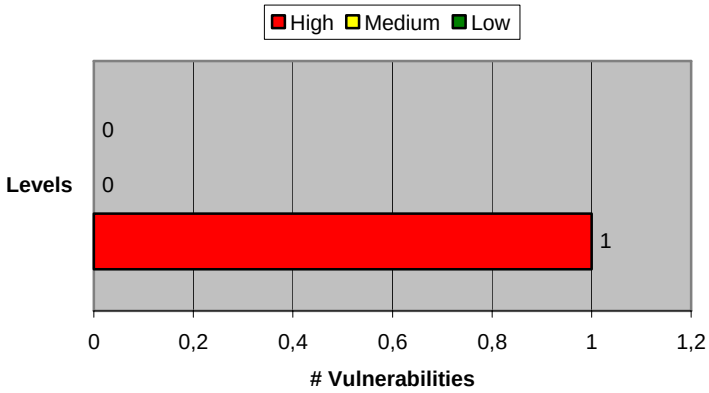
- *toroassicurazioni.it*
- *torotarga-assicurazioni.it*
- *torotarga-assicurazioni.com*
- *nuovatirrena.it*

5.3.1 Summary



Main Vulnerabilities		
Name	Description	IP
SQL Injection	E' possibile eseguire *query* SQL sul database di back-end dell'applicazione. Tramite le *extended stored procedures* è inoltre possibile eseguire comandi sulla macchina con privilegi amministrativi.	151.92.154.8 151.92.154.9 151.92.154.74

5.3.2 151.92.154.8



Generali Info		
OS fingerprint	Windows 2003	
Open TCP services	Number	Service
	80	HTTP
	8080	HTTP

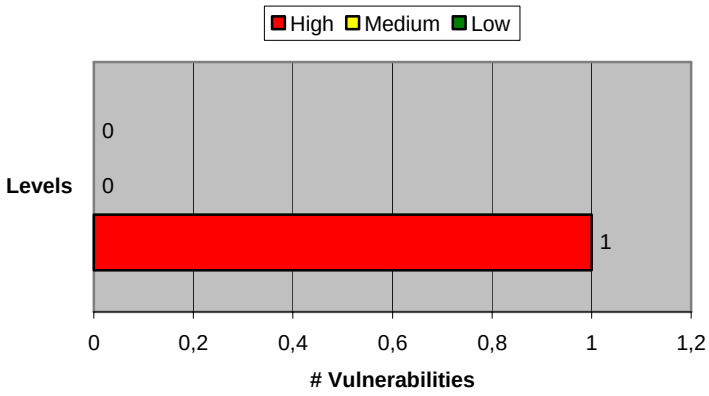
- Il servizio WEB sulla porta 80 è erogato tramite IIS 6.0
- Il servizio WEB sulla porta 8080 è erogato tramite ApacheCoyote1.1. Questo servizio risulta installato di default e apparentemente inutilizzato, e permette l'accesso (tramite password) alle componenti amministrative.
- La gestione del parametro *ID* della componente *news_mod.asp* risulta **vulnerabile ad un attacco di tipo SQL Injection**. Richidendo ad esempio l'URL

http://151.92.154.8/news_mod.asp?ID=21%27+%3B+EXEC+master.dbo.xp_cmdshell+%27cmd+%2Fc+del+c%3A%5Cfile.txt%27%3B--

è possibile effettuare la cancellazione del file "C:\file.txt" sul server SQL di back-end.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
H2	High	SQL Injection	E' possibile eseguire *query* SQL sul database di back-end dell'applicazione. Tramite le *extended stored procedures* è inoltre possibile eseguire comandi sulla macchina con privilegi amministrativi.	Sfruttando questa vulnerabilità è possibile visualizzare/modificare il contenuto del database utilizzato dall'applicazione (che potrebbe anche essere condiviso con altre applicazioni). Inoltre, la possibilità di eseguire comandi sulla macchina ha una serie di ovvie implicazioni, fra cui, ad esempio, la possibilità di interrompere il servizio.	Per eliminare la vulnerabilità è necessaria la riscrittura del codice di interfacciamento fra le pagine WEB e il database SQL. Come ulteriore soluzione è possibile l'inserimento di un *application firewall* a monte del *web server*. Le due soluzioni non sono mutuamente esclusive.

5.3.3 151.92.154.9



Generali Info		
OS fingerprint	Windows 2003	
Open TCP services	Number	Service
	80	HTTP
	8080	HTTP

- Il servizio WEB sulla porta 80 è erogato tramite IIS 6.0
- Il servizio WEB sulla porta 8080 è erogato tramite ApacheCoyote1.1. Questo servizio risulta installato di default e apparentemente inutilizzato, e permette l'accesso (tramite password) alle componenti amministrative.
- La gestione del parametro *ID* della componente *news_mod.asp* risulta **vulnerabile ad un attacco di tipo SQL Injection**. Richidendo ad esempio l'URL

http://151.92.154.9/news_mod.asp?ID=21%27+%3B+EXEC+master.dbo.xp_cmdshell+%27cmd+%2Fc+del+c%3A%5Cfile.txt%27%3B--

è possibile effettuare la cancellazione del file "C:\file.txt" sul server SQL di back-end.

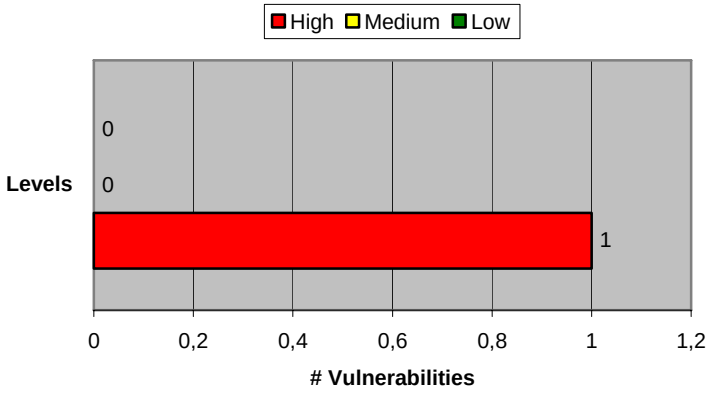
Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
H2	High	SQL Injection	E' possibile eseguire *query* SQL sul database di back-end dell'applicazione. Tramite le *extended stored procedures* è inoltre possibile eseguire comandi sulla macchina con privilegi amministrativi.	Sfruttando questa vulnerabilità è possibile visualizzare/modificare il contenuto del database utilizzato dall'applicazione (che potrebbe anche essere condiviso con altre applicazioni). Inoltre, la possibilità di eseguire comandi sulla macchina ha una serie di ovvie implicazioni, fra cui, ad esempio, la possibilità di interrompere il servizio.	Per eliminare la vulnerabilità è necessaria la riscrittura del codice di interfacciamento fra le pagine WEB e il database SQL. Come ulteriore soluzione è possibile l'inserimento di un *application firewall* a monte del *web server*. Le due soluzioni non sono mutuamente esclusive.

5.3.4 151.92.154.69

Generali Info		
OS fingerprint	Windows 2003	
Open TCP services	Number	Service
	80	HTTP
	81	HTTP

- Il servizio WEB viene erogato tramite IIS 6.0

5.3.5 151.92.154.74



Generali Info		
OS fingerprint	Windows 2003	
Open TCP services	Number	Service
	80	HTTP
	81	HTTP

- Il servizio WEB è erogato tramite IIS 6.0
- All'URL http://151.92.154.74/admin/admin.asp e' possibile accedere (tramite password) alle componenti amministrative di COLTURA. Questo risulta essere un sistema per la gestione dei contenuti WEB. Tale servizio non dovrebbe essere accessibile dall'esterno (anche se protetto da password).
- La gestione del parametro *IDCAT* della componente *index.asp* (utilizzata per il *browsing* del sito) risulta **vulnerabile ad un attacco di tipo SQL Injection**.
  Richidendo ad esempio l'URL

http://www.toroassicurazioni.it/index.asp?IDCAT=1%3B+EXEC+master.dbo.xp_cmdshell+%27cmd+%2Fc+del+c%3A%5Cfile.txt%27%3B--

è possibile effettuare la cancellazione del file “C:\file.txt” sul server SQL di back-end.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
H2	High	SQL Injection	E’ possibile eseguire *query* SQL sul database di back-end dell’applicazione. Tramite le *extended stored procedures* è inoltre possibile eseguire comandi sulla macchina con privilegi amministrativi.	Sfruttando questa vulnerabilità è possibile visualizzare/modificare il contenuto del database utilizzato dall’applicazione (che potrebbe anche essere condiviso con altre applicazioni). Inoltre, la possibilità di eseguire comandi sulla macchina ha una serie di ovvie implicazioni, fra cui, ad esempio, la possibilità di interrompere il servizio.	Per eliminare la vulnerabilità è necessaria la riscrittura del codice di interfacciamento fra le pagine WEB e il database SQL. Come ulteriore soluzione è possibile l’inserimento di un *application firewall* a monte del *web server*. Le due soluzioni non sono mutuamente esclusive.

5.3.6 151.92.154.185

Generali Info		
OS fingerprint	Windows 2003	
Open TCP services	Number	Service
	80	HTTP
	81	HTTP

- Il servizio WEB viene erogato tramite IIS 6.0

5.3.7 151.92.154.186

Generali Info		
OS fingerprint	Windows 2003	
Open TCP services	Number	Service
	80	HTTP
	81	HTTP

- Il servizio WEB viene erogato tramite IIS 6.0

5.4 Reti rimanenti

In seguito al processo di identificazione delle sottoreti del Cliente, è stato possibile individuare le seguenti subnet che, in seguito ad uno *scanning* puntuale degli indirizzi, non hanno rivelato macchine o servizi attivi (o quantomeno raggiungibili dalla rete di Hacking Team da cui è stata effettuata la scansione).

- AUGUSTATO1-NET `[194.185.201.176 - 194.185.201.191]`
- TORO1-IT `[62.123.148.0 - 62.123.148.127]`

6 Ethical Hacking interno

L'attività di *ethical hacking interno,* svolta da Hacking Team, ha avuto come oggetto di analisi le macchine (server ed apparati) facenti parte della rete interna del cliente e, pertanto, raggiungibili solo dall'interno della rete stessa. Questa fase dell'attività è stata quindi svolta dagli uffici del cliente.

Il cliente ha indicato gli indirizzi dei server collocati sulla rete interna da analizzare, senza però fornire ulteriori informazioni riguardo ai servizi esposti o alle configurazioni presenti sugli apparati.

Per una più facile consultazione, di seguito saranno presentati i risultati ottenuti aggregando gli indirizzi per classi di appartenenza.

6.1 Rete [10.36.112.0 – 10.36.112.255]

6.1.1 10.36.112.9

- High: 1
- Medium: 0
- Low: 0

Vulnerabilities				
Level	Name	Description	Threat	Fix
H3 High	Vulnerabilità RPC di Windows (BID 8205)	Il servizio Remote Procedure Call di Windows risulta vulnerabile ad un attacco remoto che permette di ottenere privilegi SYSTEM sulla macchina vittima	Un attaccante in grado di sfruttare questa vulnerabilità può ottenere accesso con privilegi elevati a tutte le risorse del sistema vulnerabile	Aggiornare il sistema operativo con i fix forniti da Microsoft

6.1.2 10.36.112.21

- High: 1
- Medium: 0
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
H3 High	Vulnerabilità RPC di Windows (BID 8205)	Il servizio Remote Procedure Call di Windows risulta vulnerabile ad un attacco remoto che permette di ottenere privilegi SYSTEM sulla	Un attaccante in grado di sfruttare questa vulnerabilità può ottenere accesso con privilegi elevati a tutte le risorse del sistema	Aggiornare il sistema operativo con i fix forniti da Microsoft

		macchina vittima	vulnerabile	
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

6.1.3 10.36.112.32

- High: 1
- Medium: 0
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
H3 High	Vulnerabilità RPC di Windows (BID 8205)	Il servizio Remote Procedure Call di Windows risulta vulnerabile ad un attacco remoto che permette di ottenere privilegi SYSTEM sulla macchina vittima	Un attaccante in grado di sfruttare questa vulnerabilità può ottenere accesso con privilegi elevati a tutte le risorse del sistema vulnerabile	Aggiornare il sistema operativo con i fix forniti da Microsoft
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

6.1.4 10.36.112.42

- High: 1
- Medium: 0
- Low: 0

Vulnerabilities				
Level	Name	Description	Threat	Fix
H3 High	Vulnerabilità RPC di Windows (BID 8205)	Il servizio Remote Procedure Call di Windows risulta vulnerabile ad un attacco remoto che permette di ottenere privilegi SYSTEM sulla macchina vittima	Un attaccante in grado di sfruttare questa vulnerabilità può ottenere accesso con privilegi elevati a tutte le risorse del sistema vulnerabile	Aggiornare il sistema operativo con i fix forniti da Microsoft

6.1.5 10.36.112.73

- High: 1
- Medium: 0
- Low: 0

Vulnerabilities				
Level	Name	Description	Threat	Fix
H3 High	Vulnerabilità RPC di Windows (BID 8205)	Il servizio Remote Procedure Call di Windows risulta vulnerabile ad un attacco remoto che permette di ottenere privilegi SYSTEM sulla macchina vittima	Un attaccante in grado di sfruttare questa vulnerabilità può ottenere accesso con privilegi elevati a tutte le risorse del sistema vulnerabile	Aggiornare il sistema operativo con i fix forniti da Microsoft

6.1.6 10.36.112.90

- High: 2
- Medium: 1
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
H4 High	Multipli buffer overflow in Sendmail (BID: 8641, 8649, 7230, 2794, 6991)	Il demone SMTP presenta diversi buffer overflow che permettono l'esecuzione remota di comandi	Un attaccante in grado di sfruttare questa vulnerabilità può prendere possesso del sistema di posta elettronica, accedendo ad informazioni personali e riservate	Aggiornare il servizio con una versione non vulnerabile
H5 High	Multipli buffer overflow in Apache (BID: 5033, 8911)	Il server web presenta diversi buffer overflow che permettono l'esecuzione remota di comandi	Un attaccante in grado di sfruttare questa vulnerabilità può prendere possesso del sistema con i privilegi del servizio web, accedendo a tutti i contenuti delle applicazioni web presenti sul sistema	Aggiornare il servizio con una versione non vulnerabile
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere

				alle informazioni, o cambiare il nome della comunità

6.2 Rete [10.36.130.0 – 10.36.130.255]

6.2.1 10.36.130.35

- High: 0
- Medium: 0
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

6.2.2 10.36.130.36

- High: 0
- Medium: 0
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

6.3 Rete [10.36.131.0 – 10.36.131.255]

6.3.1 10.36.131.44

- High: 0
- Medium: 0

- Low: 0

6.3.2 10.36.131.51

- High: 0
- Medium: 1
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L3 Low	Information leaking	E' possibile ottenere informazioni sul sistema tramite l'url /server-status	Un attaccante può ottenere informazioni utili ad attacchi successivi	Restringere l'accesso all'url o disabilitare la funzione se non utilizzata

6.3.3 10.36.131.52

- High: 0
- Medium: 1
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L3 Low	Information leaking	E' possibile ottenere informazioni sul sistema tramite l'url /server-status	Un attaccante può ottenere informazioni utili ad attacchi successivi	Restringere l'accesso all'url o disabilitare la funzione se non utilizzata

6.3.4 10.36.131.70

- High: 1
- Medium: 1
- Low: 2

Vulnerabilities				
Level	Name	Description	Threat	Fix

H5 High	Multipli buffer overflow in Apache (BID: 5033, 8911)	Il server web presenta diversi buffer overflow che permettono l'esecuzione remota di comandi	Un attaccante in grado di sfruttare questa vulnerabilità può prendere possesso del sistema con i privilegi del servizio web, accedendo a tutti i contenuti delle applicazioni web presenti sul sistema	Aggiornare il servizio con una versione non vulnerabile
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità
L4 Low	Information leaking via SMTP	Tramite i comandi VRFY e EXPN è possibile verificare in maniera veloce e automatica l'esistenza delle caselle di posta di sistema esistenti, e visualizzare i veri destinatari delle liste di distribuzione (alias)	Un attaccante può sfruttare questa implementazione per enumerare gli utenti di sistema, in previsione di un attacco di tipo bruteforce sulle password	Configurare sendmail in maniera da bloccare i comandi VRFY e EXPN

6.3.5 10.36.131.71

- High: 1
- Medium: 1
- Low: 2

Vulnerabilities				
Level	Name	Description	Threat	Fix
H5 High	Multipli buffer overflow in Apache (BID: 5033, 8911)	Il server web presenta diversi buffer overflow che permettono l'esecuzione remota di comandi	Un attaccante in grado di sfruttare questa vulnerabilità può prendere possesso del sistema con i privilegi del servizio web, accedendo a tutti i contenuti delle applicazioni web presenti sul sistema	Aggiornare il servizio con una versione non vulnerabile
M2 Medium	Glob heap corruption vulnerability del	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione	Un attaccante in possesso di credenziali d'accesso valide può	Aggiornare il servizio con una versione non

	demone FTP (BID: 2550, 3581)	remota di comandi	prendere possesso del sistema	vulnerabile
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità
L4 Low	Information leaking via SMTP	Tramite i comandi VRFY e EXPN è possibile verificare in maniera veloce e automatica l'esistenza delle caselle di posta di sistema esistenti, e visualizzare i veri destinatari delle liste di distribuzione (alias)	Un attaccante può sfruttare questa implementazione per enumerare gli utenti di sistema, in previsione di un attacco di tipo bruteforce sulle password	Configurare sendmail in maniera da bloccare i comandi VRFY e EXPN

6.3.6 10.36.131.72

- High: 1
- Medium: 1
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
H4 High	Multipli buffer overflow in Sendmail (BID: 2794, 6991)	Il demone SMTP presenta diversi buffer overflow che permettono l'esecuzione remota di comandi	Un attaccante in grado di sfruttare questa vulnerabilità può prendere possesso del sistema di posta elettronica, accedendo ad informazioni personali e riservate	Aggiornare il servizio con una versione non vulnerabile
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

6.3.7 10.36.131.73

- High: 1
- Medium: 1
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
H4 High	Multipli buffer overflow in Sendmail (BID: 2794, 6991)	Il demone SMTP presenta diversi buffer overflow che permettono l'esecuzione remota di comandi	Un attaccante in grado di sfruttare questa vulnerabilità può prendere possesso del sistema di posta elettronica, accedendo ad informazioni personali e riservate	Aggiornare il servizio con una versione non vulnerabile
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

6.3.8 10.36.131.74

- High: 0
- Medium: 1
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L4 Low	Information leaking via SMTP	Tramite i comandi VRFY e EXPN è possibile verificare in maniera veloce e automatica l'esistenza delle caselle di posta di sistema esistenti, e visualizzare i veri destinatari delle liste di distribuzione (alias)	Un attaccante può sfruttare questa implementazione per enumerare gli utenti di sistema, in previsione di un attacco di tipo bruteforce sulle password	Configurare sendmail in maniera da bloccare i comandi VRFY e EXPN

6.3.9 10.36.131.75

- High: 0
- Medium: 1
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L4 Low	Information leaking via SMTP	Tramite i comandi VRFY e EXPN è possibile verificare in maniera veloce e automatica l'esistenza delle caselle di posta di sistema esistenti, e visualizzare i veri destinatari delle liste di distribuzione (alias)	Un attaccante può sfruttare questa implementazione per enumerare gli utenti di sistema, in previsione di un attacco di tipo bruteforce sulle password	Configurare sendmail in maniera da bloccare i comandi VRFY e EXPN

6.3.10 10.36.131.132

- High: 0
- Medium: 0
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

6.3.11 10.36.131.134

- High: 0
- Medium: 0
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola	E' possibile ottenere svariate informazioni	Restringere l'accesso al servizio

		lettura con il nome di comunità di default (public)	sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

6.3.12 10.36.131.161

- High: 0
- Medium: 0
- Low: 0

6.3.13 10.36.131.162

- High: 0
- Medium: 0
- Low: 0

6.4 Rete [10.36.133.0 – 10.36.133.255]

6.4.1 10.36.133.53

- High: 0
- Medium: 0
- Low: 0

6.4.2 10.36.133.58

- High: 0
- Medium: 0
- Low: 0

6.5 Rete [10.36.136.0 – 10.36.136.255]

6.5.1 10.36.136.25

- High: 0
- Medium: 1
- Low: 2

Vulnerabilities				
Level	Name	Description	Threat	Fix

M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità
L4 Low	Information leaking via SMTP	Tramite i comandi VRFY e EXPN è possibile verificare in maniera veloce e automatica l'esistenza delle caselle di posta di sistema esistenti, e visualizzare i veri destinatari delle liste di distribuzione (alias)	Un attaccante può sfruttare questa implementazione per enumerare gli utenti di sistema, in previsione di un attacco di tipo bruteforce sulle password	Configurare sendmail in maniera da bloccare i comandi VRFY e EXPN

6.5.2 10.36.136.26

- High: 0
- Medium: 1
- Low: 2

Vulnerabilities				
Level	Name	Description	Threat	Fix
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità
L4 Low	Information leaking via SMTP	Tramite i comandi VRFY e EXPN è possibile verificare in maniera veloce e automatica l'esistenza delle caselle di posta di sistema esistenti, e visualizzare i veri destinatari delle liste di distribuzione (alias)	Un attaccante può sfruttare questa implementazione per enumerare gli utenti di sistema, in previsione di un attacco di tipo bruteforce sulle password	Configurare sendmail in maniera da bloccare i comandi VRFY e EXPN

6.6 Rete [10.36.254.0 – 10.36.254.255]

6.6.1 10.36.254.65

- High: 0
- Medium: 1
- Low: 0

Vulnerabilities				
Level	Name	Description	Threat	Fix
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile

6.6.2 10.36.254.66

- High: 1
- Medium: 1
- Low: 0

Vulnerabilities				
Level	Name	Description	Threat	Fix
H5 High	Multipli buffer overflow in Apache (BID: 5033, 8911)	Il server web presenta diversi buffer overflow che permettono l'esecuzione remota di comandi	Un attaccante in grado di sfruttare questa vulnerabilità può prendere possesso del sistema con i privilegi del servizio web, accedendo a tutti i contenuti delle applicazioni web presenti sul sistema	Aggiornare il servizio con una versione non vulnerabile
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile

7 Ethical Hacking agenziale

7.1 Descrizione

L'attività di *ethical hacking agenziale,* svolta da Hacking Team, ha analizzato le interazioni possibili tra una postazione agenziale e la rete interna del cliente. Questa fase dell'attività è stata quindi svolta da una "postazione tipo" di un'agenzia fisicamente collocata all'interno dagli uffici del cliente.

Il cliente ha indicato gli indirizzi teoricamente raggiungibili dalla postazione d'agenzia e ha fornito un file .pac contente la gestione dei proxy e degli indirizzi direttamente raggiungibili da quest'ultima senza aggiungere però dettagli riguardo ai servizi esposti. Questo vuol dire in sostanza che gli attacchi effettuati sono similabili all'azione di una persona né dipendente di agenzia né completamente estranea all'ambiente.

L'attività comprendeva anche un test di una sottorete interna non direttamente gestita dal Cliente su cui è stato fatto solamente un controllo sulla presenza di eventuali firewall per non creare disservizi o problemi al gestore della suddetta rete.

Per una più facile consultazione, di seguito saranno presentati i risultati ottenuti aggregando gli indirizzi per classi di appartenenza.

7.2 Rete [62.123.148.0-62.123.148.127]

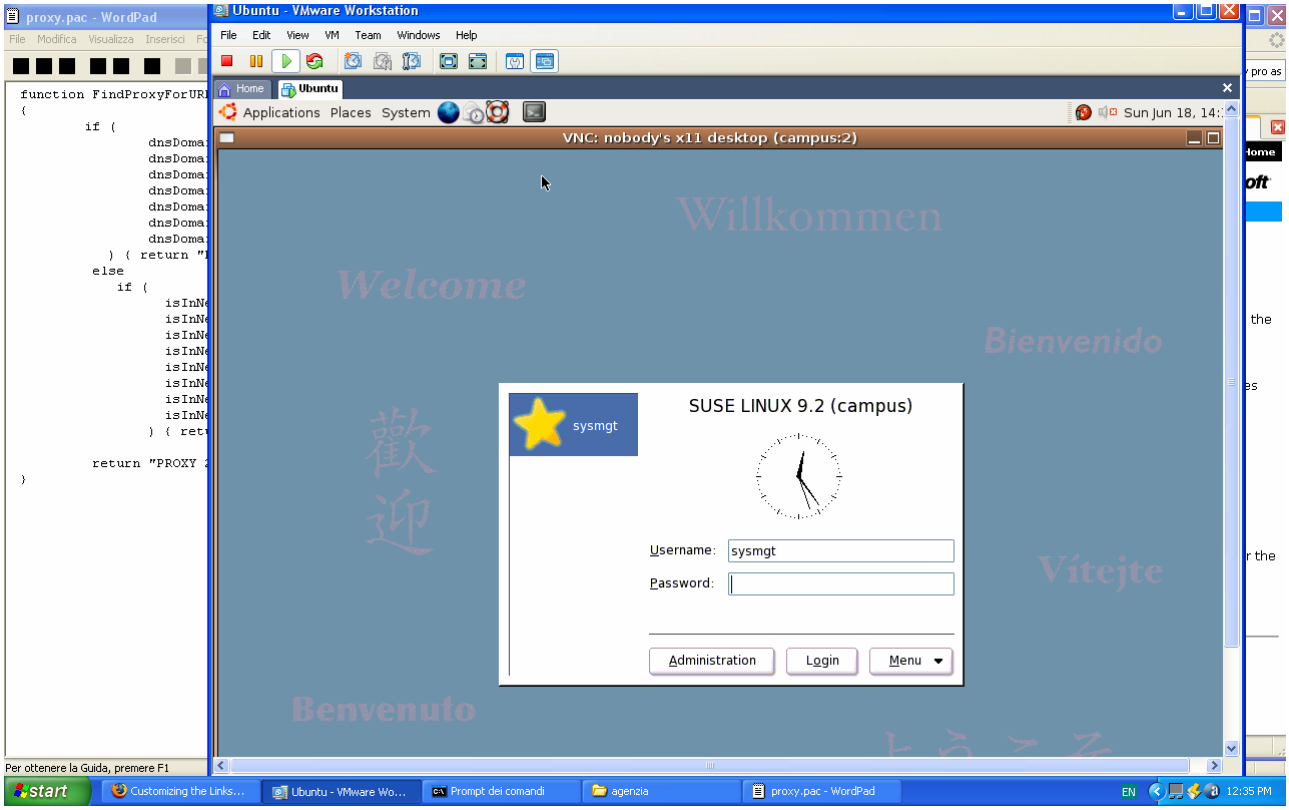
7.2.1 62.123.148.10

- High: 0
- Medium: 2
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
M3 Medium	VNC without password	Il server VNC e' senza password	Un attaccante potrebbe avere accesso alla macchina dopo che l'utente reale ha avuto accesso alla stessa	Proteggere le connessioni VNC con una password
L2	Readonly SNMP	E' presente il servizio	E' possibile ottenere	Restringere

Low	community	SNMP accessibile in sola lettura con il nome di comunità di default (public)	svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

Evidenza vulnerabilità:



7.2.2 62.123.48.62

- High: 1
- Medium: 0
- Low: 0

Vulnerabilities				
Level	Name	Description	Threat	Fix
H3 High	Vulnerabilità RPC di Windows (BID 8205)	Il servizio Remote Procedure Call di Windows risulta vulnerabile ad un attacco remoto che permette di ottenere privilegi SYSTEM sulla macchina vittima	Un attaccante in grado di sfruttare questa vulnerabilità può ottenere accesso con privilegi elevati a tutte le risorse del sistema vulnerabile	Aggiornare il sistema operativo con i fix forniti da Microsoft

7.3 Rete [10.36.0.0 – 10.36.255.255]

Quasi la totalita' delle reti non è raggiungibile da questa postazione grazie a firewall che bloccano le richieste di connessione rispondendo con un icmp host unreachable.

Il firewall e' stato analizzato ed e' stato trovato vulnerabile a causa della mancata configurazione delle password dell'apparato.

7.3.1 Cisco Firewall ip: *10.36.3.133*

Vulnerabilities				
Level	Name	Description	Threat	Fix
H6 High	Default Password on Cisco Firewall	Non è stata riconfigurata la password di default con privilegi di amministrazione del cisco firewall. Default passwd: username: cisco passwd: cisco	Un attaccante in grado di autenticarsi con queste credenziali potrebbe prenderne completamente il controllo riuscendo così a raggiungere gran parte della rete interna del Cliente.	Impostare una password sicura sul device vulnerabile.

Evidenze:

Configurazione del router corrente:

```
Using 10707 out of 524288 bytes
!
! Last configuration change at 12:44:01 CEST Tue May 23 2006 by gtee1
! NVRAM config last updated at 12:44:02 CEST Tue May 23 2006 by gtee1
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log datetime localtime
service password-encryption
!
hostname SW-DMZAGA
!
logging rate-limit 10000
no logging console
enable password 7 00071A150754
!
username gice1 password 7 111D0B4B041B0F0D082E2460786274
username gtee1 password 7 15101D1F4A737E6579
username gtei3 password 7 13170306195D5D727B
aaa new-model
aaa authentication login default local
!
```

```
aaa session-id common
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 1:00 last Sun Oct 1:00
switch 1 provision ws-c3750g-24ts
vtp domain DMZHI
vtp mode transparent
ip subnet-zero
ip routing
no ip domain-lookup
ip domain-name gruppotoro.it
!
!
!
crypto pki trustpoint TP-self-signed-3280167296
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3280167296
 revocation-check none
 rsakeypair TP-self-signed-3280167296
!
!
crypto ca certificate chain TP-self-signed-3280167296
 certificate self-signed 01 nvram:SW-DMZAGAgru#7401.cer
!
!
no file verify auto
!
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 8,64,184 priority 16384
!
vlan internal allocation policy ascending
!
vlan 64
 name VPNAGE
!
vlan 85
 name Vlan-Internet-FWeb
!
vlan 101
 name ispett_presidi
!
vlan 169
 name BackboneAtlanet
!
vlan 184
 name DMZAGEHI
!
vlan 258
 name fornitori
!
vlan 431
 name Vlan-Internet-Atl
!
vlan 515
 name VETRINA
!
vlan 840
 name RAS
!
!
interface GigabitEthernet1/0/1
 description collegamento interfaccia esterna CheckPointA
```

```
 switchport access vlan 64
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description collegamento interfaccia interna CheckPointA
 switchport access vlan 184
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 description collegamento verso RadwareA
 switchport access vlan 184
 switchport mode access
 duplex full
 speed 1000
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 description interfaccia verso VPN-Age server ftp-agenzie
 switchport access vlan 184
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 description test webseal1 esposto vpn age per test probl i.e. 6.0-wsd
 switchport access vlan 184
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/6
 description per iasi proxy gw age
 switchport access vlan 184
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/7
 description per iasi proxy gw age
 switchport access vlan 184
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
 description interf vs rasforna vlan ispett,ras,fornit
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 258,840
 switchport mode trunk
 shutdown
!
interface GigabitEthernet1/0/11
 description PC esterno
 switchport access vlan 169
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/12
 description PC test posto tra FW e Radware
 switchport access vlan 184
 switchport mode access
```

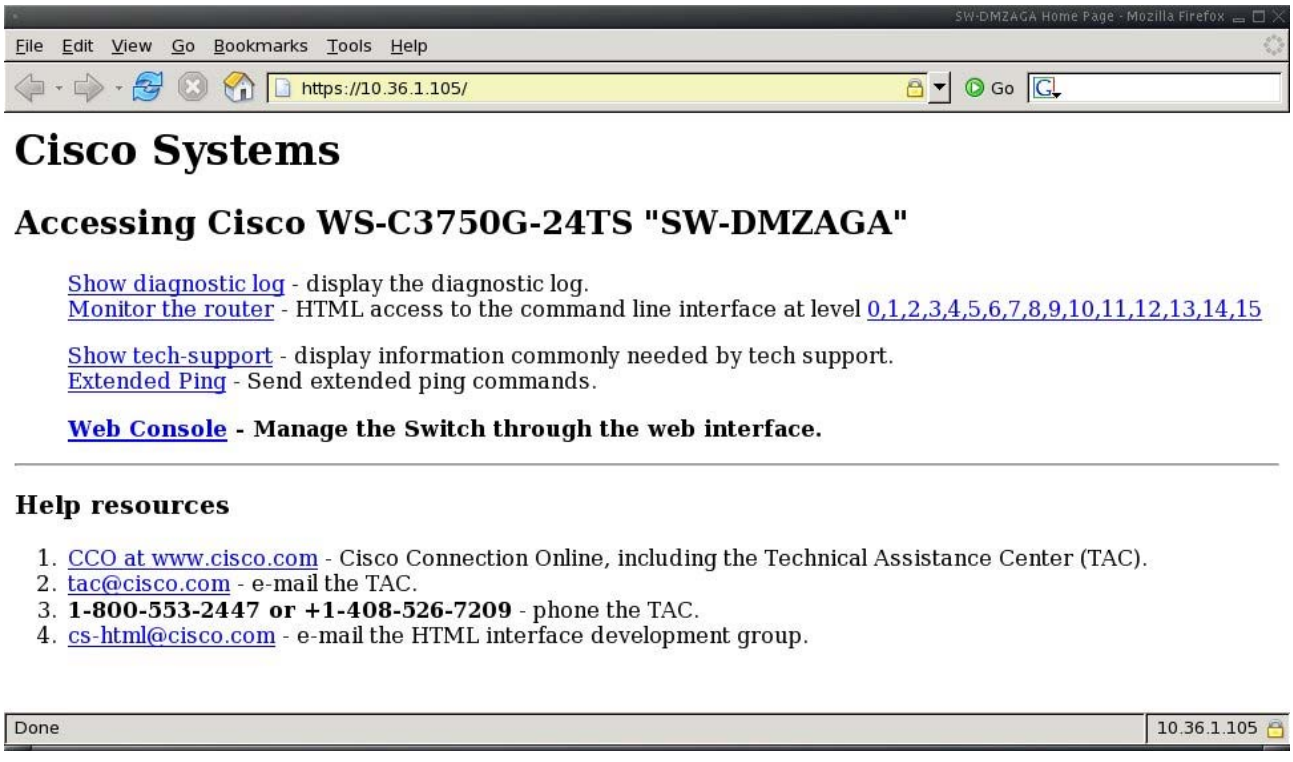
```
 spanning-tree portfast
!
interface GigabitEthernet1/0/13
 description porta connessione vs siti vetrina/dmz gvs
 switchport access vlan 515
 switchport mode access
 duplex full
 speed 100
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
 description ingresso su G400B Link Internet FW
 switchport access vlan 85
!
interface GigabitEthernet1/0/20
 description description ingresso Link Internet FWeb
 switchport access vlan 85
 switchport mode access
 duplex full
 speed 100
!
interface GigabitEthernet1/0/21
 description porta com vs sw dmzagloa per management
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode trunk
!
interface GigabitEthernet1/0/22
 description Collegamento con C3550A per trasporto vlan Internet
 switchport access vlan 431
 switchport mode access
!
interface GigabitEthernet1/0/23
 description collegamento con SW-DMZAGB per trasporto vlan esterne al firewall
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 64,85,169,258,431,515,840
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 description collegamento con SW-DMZAGB per trasporto vlan interne al firewall
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,101,184
 switchport mode trunk
!
interface GigabitEthernet1/0/25
 description Trunk di connessione v.so Backbone Atlanet VPN agenzie-Ispett.-Forn
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 169
 switchport mode trunk
!
interface GigabitEthernet1/0/26
 description trunk per Backup Atlanet
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 169,431
```

```
 switchport mode trunk
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface Vlan1
 description vlan di management
 ip address 10.36.1.105 255.255.255.240
 ip access-group 101 in
!
interface Vlan64
 ip address 10.36.3.69 255.255.255.248
 standby authentication md5 key-string 7 071B2E5E41440F09161C5D58
 standby 64 ip 10.36.3.68
 standby 64 priority 120
 standby 64 preempt
!
interface Vlan169
 description Layer3 verso Backbone Atlanet VPNAgenzie
 ip address 10.36.3.166 255.255.255.240
 standby 169 ip 10.36.3.165
 standby 169 priority 120
 standby 169 preempt
 standby 169 authentication md5 key-string 7 00301C140B0A5D5F
!
interface Vlan515
 ip address 10.36.3.133 255.255.255.248
 standby authentication md5 key-string 7 030C481916392D4D4051
 standby 8 ip 10.36.3.132
 standby 8 priority 120
 standby 8 preempt
!
ip classless
ip route 10.36.112.8 255.255.255.255 10.36.3.65
ip route 10.36.113.0 255.255.255.0 10.36.3.65
ip route 10.36.113.8 255.255.255.255 10.36.1.97
ip route 10.36.113.39 255.255.255.255 10.36.3.65
ip route 10.36.113.160 255.255.255.255 10.36.1.97
ip route 10.36.113.169 255.255.255.255 10.36.1.97
ip route 10.36.113.244 255.255.255.255 10.36.1.97
ip route 10.36.114.0 255.255.255.0 10.36.3.65
ip route 10.36.130.34 255.255.255.255 10.36.3.65
ip route 10.36.131.1 255.255.255.255 10.36.1.98
ip route 10.36.131.3 255.255.255.255 10.36.1.98
ip route 10.36.131.50 255.255.255.255 10.36.3.65
ip route 10.36.131.51 255.255.255.255 10.36.3.65
ip route 10.36.131.52 255.255.255.255 10.36.3.65
ip route 10.36.131.65 255.255.255.255 10.36.1.97
ip route 10.36.133.11 255.255.255.255 10.36.1.97
ip route 10.36.133.12 255.255.255.255 10.36.1.97
ip route 10.36.136.20 255.255.255.255 10.36.3.65
ip route 10.36.137.20 255.255.255.255 10.36.3.65
ip route 10.36.137.50 255.255.255.255 10.36.3.65
ip route 10.41.128.0 255.255.128.0 10.36.3.161
ip route 10.49.0.0 255.255.0.0 10.36.3.161
ip route 10.49.0.0 255.255.240.0 10.36.3.65
ip route 10.70.0.15 255.255.255.255 10.36.3.65
ip route 10.70.0.16 255.255.255.255 10.36.3.65
ip route 10.70.128.0 255.255.255.0 10.36.3.65
ip route 10.70.224.0 255.255.240.0 10.36.3.161
ip route 62.123.148.0 255.255.255.128 10.36.3.65
ip route 151.88.0.0 255.255.0.0 10.36.3.129
```

```
ip route 151.92.0.0 255.255.0.0 10.36.3.129
ip route 192.168.146.84 255.255.255.255 10.36.3.65
ip route 192.168.146.85 255.255.255.255 10.36.3.65
no ip http server
ip http secure-server
!
!
logging 10.36.133.12
access-list 50 permit 10.36.113.8
access-list 50 permit 10.36.113.39
access-list 50 permit 10.36.133.11
access-list 50 permit 10.36.113.244
access-list 50 permit 10.36.115.169
access-list 50 permit 10.36.113.160
access-list 99 permit 10.36.133.11
access-list 99 permit 10.36.133.12
access-list 99 permit 10.36.131.65
access-list 101 permit ip host 10.36.113.8 any
access-list 101 permit ip host 10.36.113.39 any
access-list 101 permit ip host 10.36.113.160 any
access-list 101 permit ip host 10.36.133.11 any
access-list 101 permit ip host 10.36.133.12 any
access-list 101 permit ip host 10.36.131.1 any
access-list 101 permit ip host 10.36.131.3 any
access-list 101 permit ip host 10.36.131.65 any
access-list 101 permit ip host 10.36.113.244 any
access-list 101 permit ip host 10.36.115.169 any
access-list 111 permit udp 10.70.230.0 0.0.0.255 host 151.88.177.50 eq 38293 log-input
access-list 111 permit udp 10.70.230.0 0.0.0.255 host 151.88.177.51 eq 2967 log-input
access-list 111 permit udp 10.70.231.0 0.0.0.255 host 151.88.177.50 eq 38293 log-input
access-list 111 permit udp 10.70.231.0 0.0.0.255 host 151.88.177.51 eq 2967 log-input
access-list 111 permit udp 10.70.230.0 0.0.0.255 host 151.88.177.50 log-input
access-list 111 permit udp 10.70.231.0 0.0.0.255 host 151.88.177.51 log-input
access-list 111 permit ip any any
access-list 112 permit udp 151.88.177.0 0.0.0.255 10.70.230.0 0.0.0.255 eq 2967 log-input
access-list 112 permit udp 151.88.177.0 0.0.0.255 10.70.231.0 0.0.0.255 eq 38293 log-
input
access-list 112 permit udp 151.88.177.0 0.0.0.255 10.70.230.0 0.0.0.255 log-input
access-list 112 permit udp 151.88.177.0 0.0.0.255 10.70.231.0 0.0.0.255 log-input
access-list 112 permit ip any any
arp 10.36.3.65 0100.5e24.0341 ARPA
snmp-server community toro-snmp RO 99
snmp-server community T0r0 RW 99
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps cluster
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps MAC-Notification
snmp-server enable traps copy-config
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
```

```
snmp-server host 10.36.133.12 T0r0
radius-server source-ports 1645-1646
!
control-plane
!
!
line con 0
line vty 0 4
 access-class 50 in
 transport input ssh
line vty 5 15
 access-class 50 in
 transport input ssh
!
mac-address-table static 0100.5e7b.9401 vlan 184 interface GigabitEthernet1/0/2
GigabitEthernet1/0/24
mac-address-table static 0100.5e24.0341 vlan 64 interface GigabitEthernet1/0/1
GigabitEthernet1/0/23
ntp clock-period 36028750
ntp source Vlan1
ntp server 10.36.131.3
ntp server 10.36.131.1 prefer
!
end
```

Screenshot:



7.3.2 www.gruppotoro.net

- High: 0
- Medium: 1
- Low: 1

Vulnerabilities				
Level	Name	Description	Threat	Fix
M2 Medium	Glob heap corruption vulnerability del demone FTP (BID: 2550, 3581)	Il server FTP presenta una vulnerabilità che può permettere l'esecuzione remota di comandi	Un attaccante in possesso di credenziali d'accesso valide può prendere possesso del sistema	Aggiornare il servizio con una versione non vulnerabile
L2 Low	Readonly SNMP community	E' presente il servizio SNMP accessibile in sola lettura con il nome di comunità di default (public)	E' possibile ottenere svariate informazioni sul sistema vittima, sia di tipo infrastrutturale, sia di tipo statistico	Restringere l'accesso al servizio solo dagli indirizzi che effettivamente devono accedere alle informazioni, o cambiare il nome della comunità

8 Piano dei lavori

8.1 Strategia di Fixing

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 remoto VNC senza richiesta di credenziali, con appropriato piano di cambio periodico e *password management*.	M3

8	Controllo, sistemazione e pulizia della configurazione delle macchine.	L2 L3 L4

8.2 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.

9 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.

9.1 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.

9.2 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 5.3.1).
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.

9.3 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 5.2.3); 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.