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
//	//	//
//	//	//

INFORMAZIONI		
Data di Emissione	08 Giugno 2006	
Versione	0.1 (BOZZA)	
Tipologia Documento	Documento di Progetto	
Numero di Protocollo	//	
Numero Pagine	27	
Numero Allegati	0	
Descrizione Allegati	1	//
	2	//
Redatto da	Marco Valleri	
Approvato da	Gianluca Vadruccio	

INDICE

1 Introduzione

1.1 Obiettivo del lavoro

1.2 Vincoli e limiti del lavoro svolto

1.3 Ambito e perimetro del lavoro

1.4 Struttura del documento

2 Principi generali

3 Metodologia

4 Analisi topologica ed architetturale

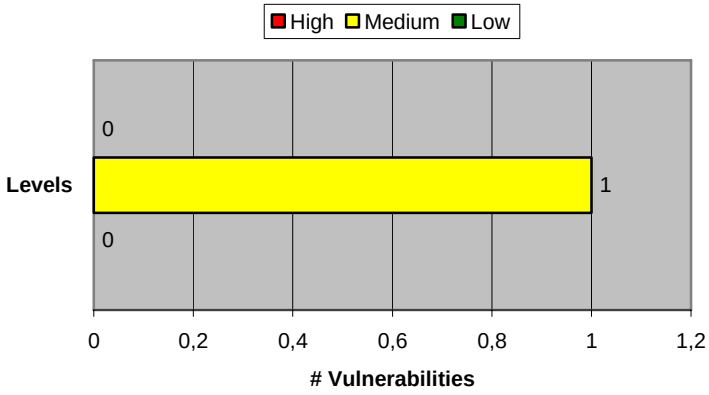
4.1 Studio rete esterna

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

4.3 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

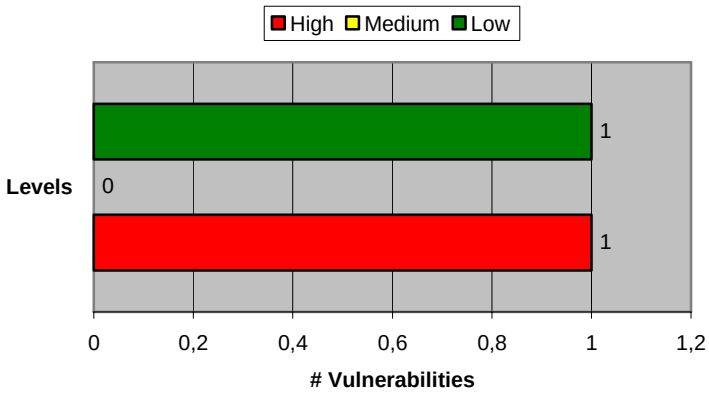
5.2 Rete [194.247.182.64 - 194.247.182.95]

5.2.1 Descrizione

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

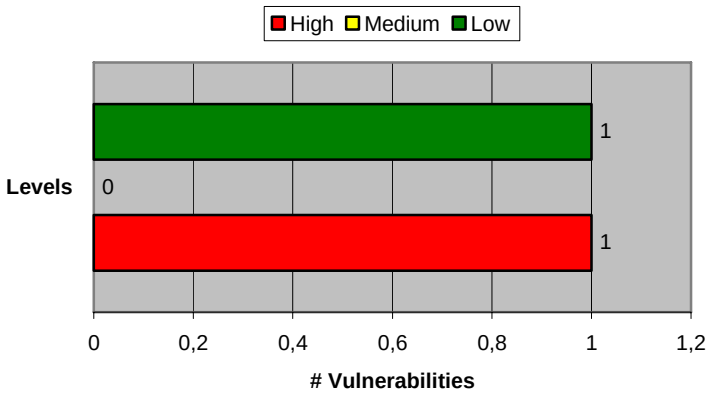
Almeno una delle macchine ospitate da questa sottorete è risultata collegata direttamente anche alla rete interna del Cliente (o quantomeno non è stato individuato nessun dispositivo di filtraggio del traffico tra essa e la rete interna). Questo ha permesso, in seguito alla compromissione della macchina, di avere accesso ai sistemi e ai servizi della rete interna (vedere paragrafi 4.3 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 4.3 e 8)

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

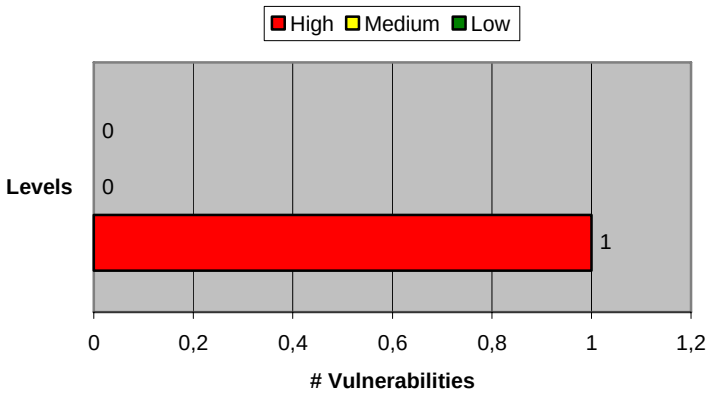
- Il servizio WEB è erogato tramite IIS 6.0.

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:

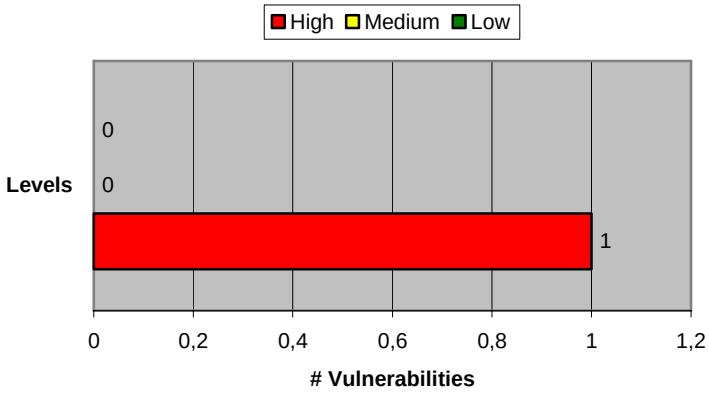
- *toroassicurazioni.it*
- *torotarga-assicurazioni.it*
- *torotarga-assicurazioni.com*
- *nuovatirrena.it*

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

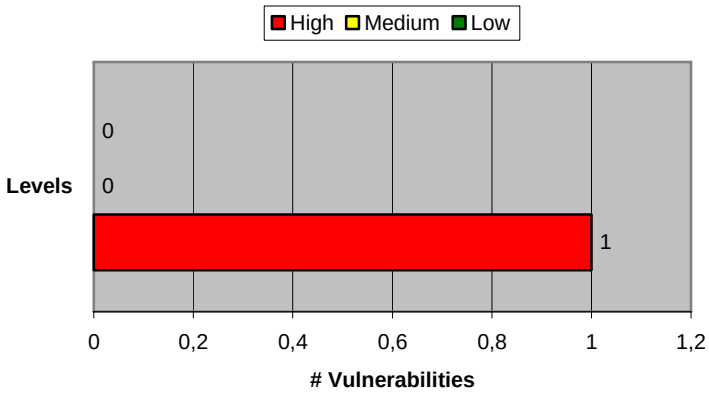
- Il servizio WEB sulla porta 80 è erogato tramite IIS 6.0
- Il servizio WEB sulla porta 8080 è erogato tramite ApacheCoyote1.1. Questo servizio risulta installato di default e apparentemente inutilizzato, e permette l'accesso (tramite password) alle componenti amministrative.
- La gestione del parametro *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.

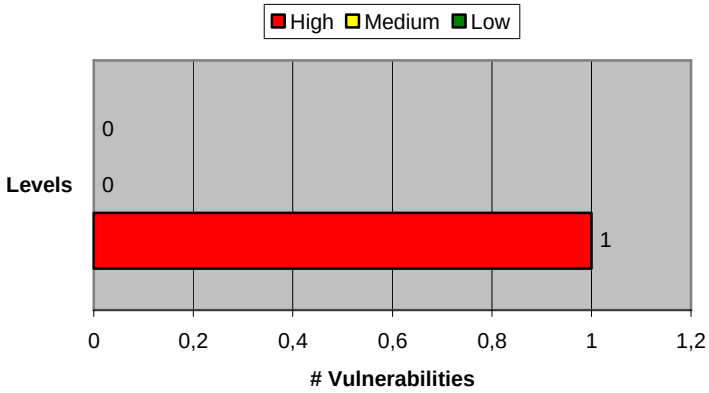
Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
H2	High	SQL Injection	E' possibile eseguire *query* SQL sul database di back-end dell'applicazione. Tramite le *extended stored procedures* è inoltre possibile eseguire comandi sulla macchina con privilegi amministrativi.	Sfruttando questa vulnerabilità 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**.

  Richiedendo 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).

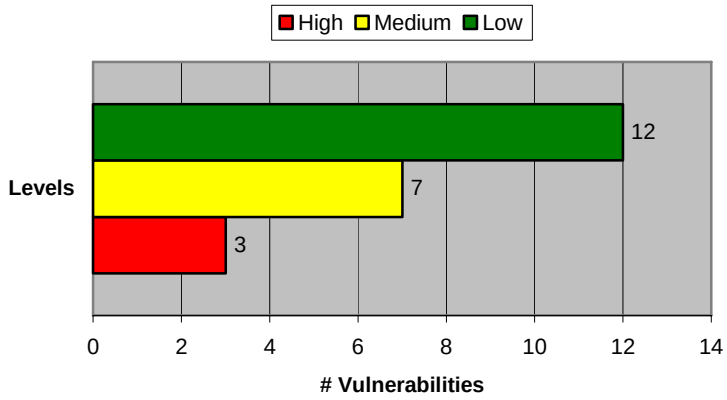
- AUGUSTATO1-NET `[194.185.201.176 - 194.185.201.191]`
- TORO1-IT `[62.123.148.0 - 62.123.148.127]`

6 Ethical Hacking interno

6.1 Rete 1

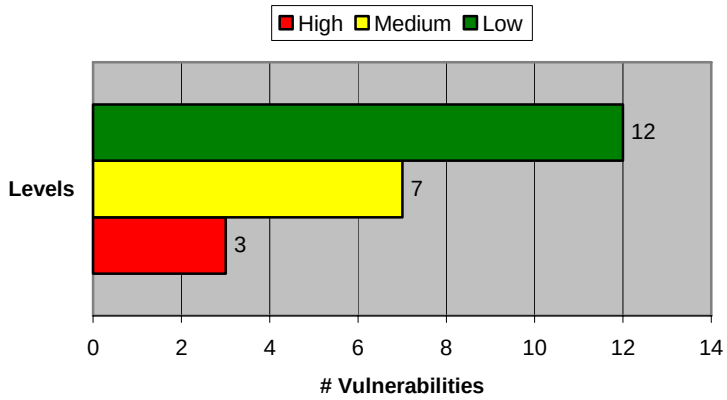
6.1.1 Descrizione

6.1.2 Summary



Main Vulnerabilities		
Name	Description	IP

6.1.3 IP 1



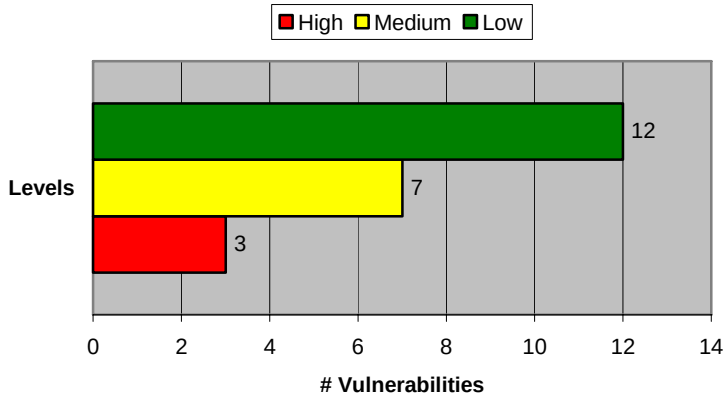
Generali Info		
OS fingerprint		
Open TCP services	Number	Service

Open UDP services	Number	Service

Descrizione sommaria della macchina.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix

6.1.4 IP 2



Generali Info		
OS fingerprint		
Open TCP services	Number	Service
Open UDP services	Number	Service

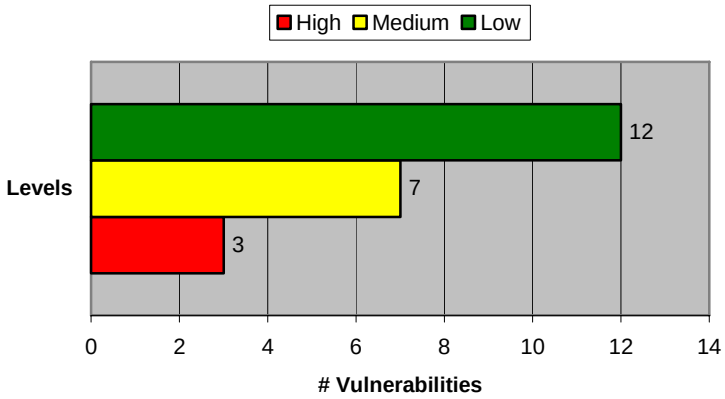
Descrizione sommaria della macchina.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix

6.2 Rete 2

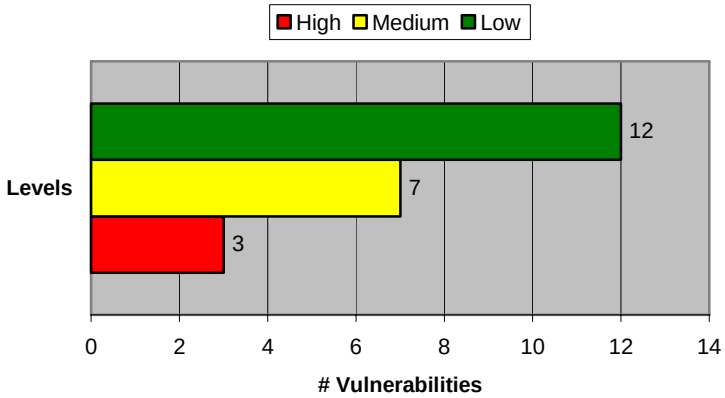
6.2.1 Descrizione

6.2.2 Summary



Main Vulnerabilities		
Name	Description	IP

6.2.3 IP 1



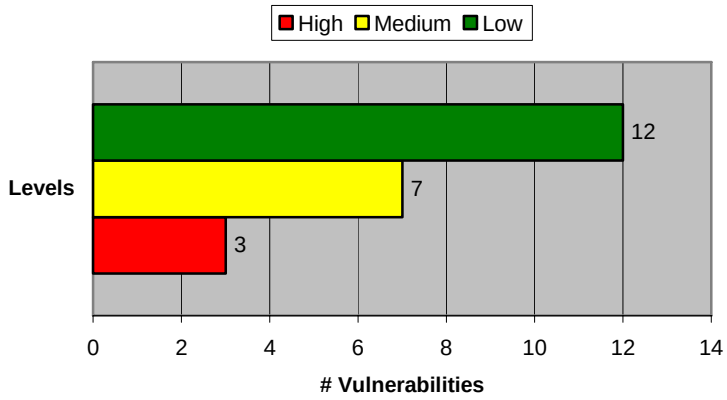
Generali Info		
OS fingerprint		
Open TCP services	Number	Service

Open UDP services	Number	Service

Descrizione sommaria della macchina.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix

6.2.4 IP 2



Generali Info		
OS fingerprint		
Open TCP services	Number	Service
Open UDP services	Number	Service

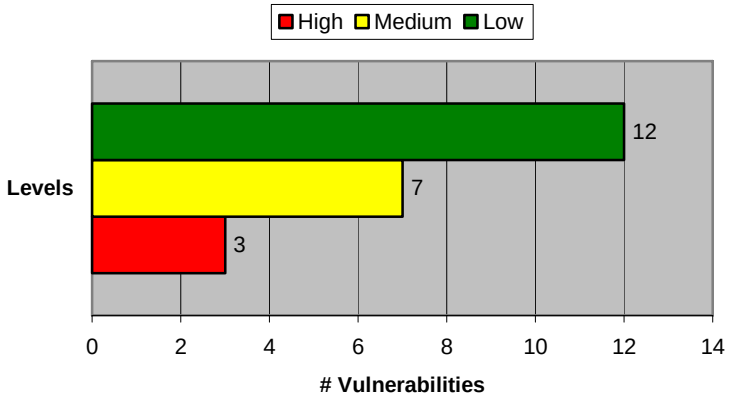
Descrizione sommaria della macchina.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix

7 Ethical Hacking agenziale

7.1 Descrizione

7.2 Vulnerabilità riscontrate



Vulnerabilities					
#n	Level	Name	Description	Threat	Fix

8 Security Plan

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 (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.	-

9 Attività consigliate