XXXX

Ethical Hacking

XXX

Hacking Team S.r.l.	http://www.hackingteam.it
Via Moscova, 13 *20124 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.66988639	*Fax +39.02.67381939*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate

INFORMAZIONI		
Data di Emissione		
Versione		
Tipologia Documento	Report attivita' di Ethical Hacking	
Numero di Protocollo		
Numero Pagine		
Numero Allegati		
Descrizione Allegati	1	
	2	
Redatto da		
Approvato da		

INDICE

1 Introduzione

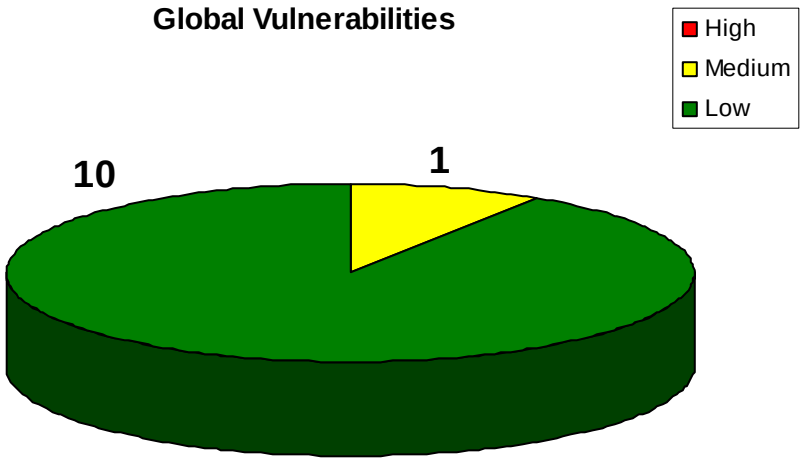
1.1 Obiettivo

Scopo del documento è quello di illustrare l'attività di *security probe* effettuata da Hacking Team S.r.l. verso i sistemi informatici appartenenti alla rete di **XXXX**.

In questo documento sono analizzate tutte le debolezze riscontrate e, nei casi in cui è possibile, sono suggerite le soluzioni più indicate a risolvere il problema in questione.

2 Executive Summary

2.1 Parte esterna



Le macchine analizzate hanno denotato un ottimo livello di sicurezza. Tuttavia, ogni singola macchina e' stata analizzata solamente in maniera puntuale (come da richiesta del Cliente) e non inquadrata nel suo contesto infrastrutturale.

Availability
➢ 1 Il servizio www.XXXXxxxx.it **potrebbe** essere reso indisponibile
Confidentiality
➢ 1 Un attaccante in grado di intercettare flussi di traffico fra i client e i web server potrebbe essere in grado di decifrare i dati protetti dalla cifratura SSL

Le pochissime vulnerabilita' riscontrate riguardano principalmente la possibilita' di decifrare flussi di traffico intercettato. L'impatto e l'effettivo coefficiente di rischio di tali vulnerabilita' e' tuttavia molto basso.

3 Principi generali

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

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.

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.

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.

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.

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.

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.

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].

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 "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.

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

4 Metodologia

Il security probe condotto da Hacking Team S.r.l. è stato effettuato all'esterno e all'interno del network di **XXXX** simulando in tutto e per tutto le attività che avrebbe compiuto un hacker. E' stato ricostruito, in altre parole, il "percorso" logico che un qualsiasi hacker percorrerebbe se volesse in qualche maniera oltrepassare le misure difensive della rete di XXXX.
Coerentemente all'approccio metodologico di riferimento illustrato di seguito, effettuando l'attacco si è per prima cosa cercato di ricostruire la topologia e le caratteristiche dei sistemi e dei siti da attaccare. In un secondo momento, tali sistemi sono stati analizzati singolarmente, e si è quindi cercato di sfruttare le debolezze presenti sugli stessi.
E' bene evidenziare che l'accesso ad una sola delle macchine da parte di un attaccante esterno, permette poi l'esposizione diretta degli altri server. L'utilizzo di un "ponte" da cui accedere alle altre macchine è una pratica tipica ed efficace per ottenere il massimo da un'attività di incursione informatica.

ANALISI NON INVASIVA

FOOTPRINTING

Questa fase ha lo scopo di raccogliere il maggior numero di informazioni sull'obiettivo che si intende attaccare senza "toccare" l'obiettivo stesso, ovvero effettuando una cosiddetta "analisi non invasiva". In particolare in questa fase è importante determinare: *domini, blocchi di rete e gli indirizzi ip dei sistemi direttamente collegati ad internet*. Gli strumenti utilizzati sono: Search Engine, server whois, database Arin/Ripe ed interrogazioni ai dns.

SCANNING

L'obiettivo dello scanning è ottenere una mappa il più dettagliata possibile del sistema da attaccare; ciò significa acquisire informazioni su quali ip dei blocchi di rete trovati nella fase precedente siano effettivamente contattabili dall'esterno (Ip discovery) e, relativamente a tali ip, scoprire che servizi abbiano attivi (Tcp/udp port scan) e che sistemi operativi posseggano. Gli

strumenti utilizzati sono: interrogazioni ICMP (gping, fping, ecc.), la scansione delle porte tcp e udp (strobe, netcat, nmap, rascan) e fingerprint dello stack (nmap, queso).

ANALISI INVASIVA

ENUMERATION

Con questa fase si inizia "l'analisi invasiva" infatti si effettuano connessioni dirette ai server ed interrogazioni esplicite, il che potrebbe (a seconda della configurazione presente sui sistemi target) originare dei logs.
Attraverso l'enumerazione si vuole giungere a identificare, sulle macchine riscontrate come raggiungibili, degli account validi (list user accounts), delle risorse condivise (list file shares) e delle applicazioni attive sulle porte in ascolto (identify application). Le tecniche utilizzate variano dai sistemi operativi delle macchine che vogliamo analizzare.

ATTACCO

GAINING ACCESS

Una volta ottenute le informazioni del punto precedente inizia il vero e proprio attacco che ha come obiettivo il riuscire ad entrare nel sistema remoto.
I metodi utilizzati anche in questo caso dipendono dal sistema operativo della macchina target, ma si basano sostanzialmente sulla ricerca di password corrispondenti agli utenti trovati (password guessing), sullo sfruttamento di errori progettuali delle applicazioni e servizi attivi sul server (buffer overflows, attacchi data driven, ecc.) o del sistema operativo stesso.

ESCALATING PRIVILEGES

L'obiettivo di questa fase è sfruttare i risultati ottenuti nella fase precedente per ottenere il pieno controllo del sistema remoto attaccato. Ciò si ottiene reperendo i files presenti sul sistema che contengono le password (/etc/passwd, SAM, ecc.) e tentando di decifrare le password in essi contenute (password cracking), oppure utilizzando appositi exploits.

CONSOLIDAMENTO

PILFERING

Se si giunge a questa fase significa che si è ottenuto il pieno controllo del sistema target. Quindi è bene valutare la configurazione del sistema stesso al fine di capire se, dove e cosa il sistema registra (logs), eventualmente si disabilita l'auditing (es. con Win NT mediante auditpol). A questo punto la macchina in oggetto può diventare un trampolino che permetta di attaccare altre macchine, di conseguenza può essere utile reperire sul file system eventuali informazioni riguardanti altri sistemi

COVERING TRACES AND CREATING BACK DOORS

Prima di abbandonare il sistema conquistato vengono cancellati gli eventuali i logs che hanno registrato la presenza clandestina e eventualmente installare trojan o back doors che consentano di rientrare facilmente sulla macchina in un secondo momento. Può essere utile anche installare tools nascosti quali sniffers o keyloggers al fine di catturare altre password del sistema locale o di altri sistemi ai quali ignari utenti si collegano dalla macchina "hackerata".

Nel caso di un attacco simulato, come quello effettuato presso la rete di XXXX, nel caso si riescano a superarne le difese **ci si fermerà comunque alla fase alla fase 5**, al fine di dimostrare l'effettiva possibilità di assumere il controllo delle macchine senza comunque apportare alcuna modifica sulle stesse.

5 Analisi topologica ed architetturale

5.1 Studio rete esterna

L'analisi delle vulnerabilita' esterne della rete **XXXX** e' stata effettuata in maniera puntuale. Le macchine indicate dal Cliente come critiche sono state testate singolarmente.
Per una topologia della rete ospitante le macchine esaminate si veda il paragrafo 6.1.1

5.2 Studio rete interna

L'analisi delle vulnerabilita' interne alla rete **XXXX** e' stata effettuata in maniera puntuale. Le macchine indicate dal Cliente come critiche sono state testate singolarmente.

5.3 Vulnerabilità architetturali

L'analisi delle vulnerabilita' esterne e interne alla rete **XXXX** e' stata effettuata in maniera puntuale. Le macchine indicate dal Cliente come critiche sono state testate singolarmente.

6 Studio esterno

6.1 Rete x.x.x.0/22

Questi sono i dati relativi alla rete, ottenibili tramite un'interrogazione al database pubblico *whois* del RIPE:

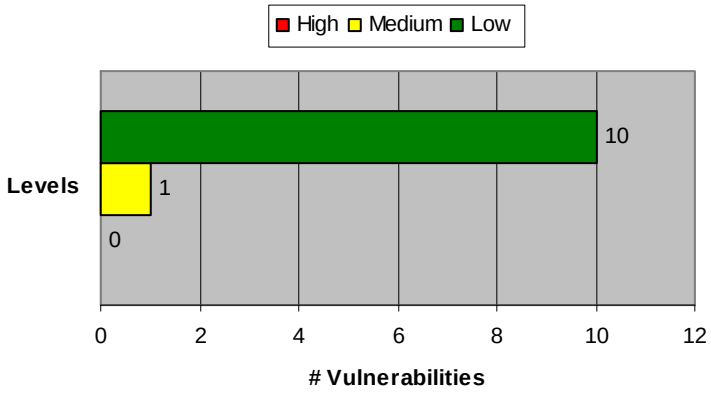
```
inetnum:        x.x.x.0 - x.x.x.255
netname:        XXXX-NET
descr:          Xxxx XXXX S.p.A. Network
country:        IT
admin-c:        AB318
tech-c:         MBS15-RIPE
rev-srv:        xxxx
rev-srv:        xx.xxxx.xx # x.x.x.1
status:         ASSIGNED PA
mnt-by:         XXXX-MNT
changed:        xxxx
changed:        xxxx
source:         RIPE
route:          x.x.x.0/22
descr:          route object for allocation release by RIPE NCC to it.XXXX
origin:         ASxxxxx
notify:         xxxx
mnt-lower:      XXXX-MNT
mnt-by:         XXXX-MNT
changed:        xxxx
source:         RIPE
role:           XXXX xxxx Staff
address:        Xxxx XXXX S.p.A.
address:        xxxx
address:        xxxx xxxx (xx)
address:        xxxx
phone:          +39 xx xxxx.1
fax-no:         +39 xx xxxxx
e-mail:         xx@XXXX.xx
admin-c:        xxxx
admin-c:        xxxx-xxxx
tech-c:         xxxx
nic-hdl:        xxxx-RIPE
changed:        xx@xx.it xxxxx
source:         RIPE
```

6.1.1 Description

Le macchine prese in esame sono raggiungibili tramite i due gateway *x.x.x.236* e *x.x.x.x.237*. A monte dei due gateway c'e' l'ISP xxxx.

L'unica eccezione e' rappresentata dalla macchina *x.x.x.106*, raggiungibile tramite l'ISP xxxx.

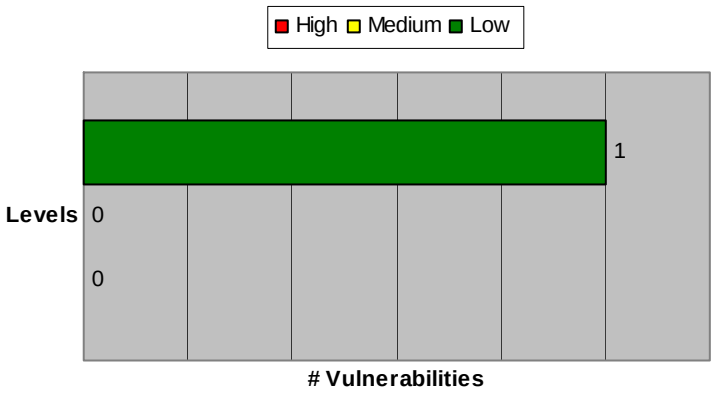
6.1.2 Summary



Main Vulnerabilities		
Name	Description	IP
SSL Downgrade	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	x.x.x.x.1 x.x.x.x.2 x.x.x.x.7 x.x.x.x.15 x.x.x.x.18 x.x.x.x.25 x.x.x.x.66 x.x.x.x.196 x.x.x.x.198
PHP4 Multiple Vulnerabilities[2]	PHP4 contiene numerosi overflow all'interno di alcune funzioni come base64_encode() e ibase_blob_get()	x.x.x.x.6

[2] Nonostante la versione di PHP risulti vulnerabile, non e' stato trovato nessun *vettore di attacco* utile all'interno delle pagine php presenti sul server. Per essere sfruttata, la vulnerabilita' richiede infatti che una delle funzioni vulnerabili venga utilizzata su dei dati inseriti dall'utente. Non e' stato possibile verificare queste condizioni sulle pagine attualmente presenti sul server, e questo rappresenta un fattore mitigante.

6.1.3 x.x.x.x.1 – www.xxxxXXXX.xxx

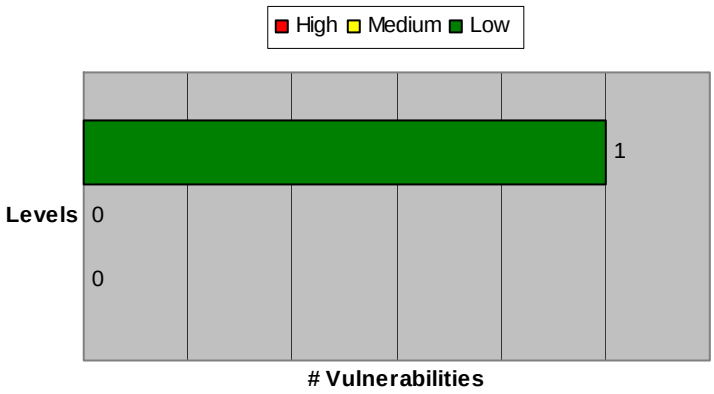


General Info		
OS fingerprint	Windows 2000	
Open TCP services	Number	Service
	443	HTTPS

- La pagina principale del sito web presenta un *redirect* verso https://www.xxxxXXXX.xx/home.html
- Analizzando gli header di risposta, il WebServer sembra essere Netscape-Enterprise/6.0

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
L2	Low	SSL Downgrade	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	Unito ad attacchi di traffic redirection (*route mangling, DNS poisoning,* etc.) potrebbe essere possibile impersonare il server verso altri client o decifrare il flusso di dati.	Se non utilizzati per ragioni di retrocompatibilita', disabilitare SSLv2 e l'utlizzo di chiavi minori di 128bit.

6.1.4 x.x.x.x.2 – www.xxxxXXXX.xx

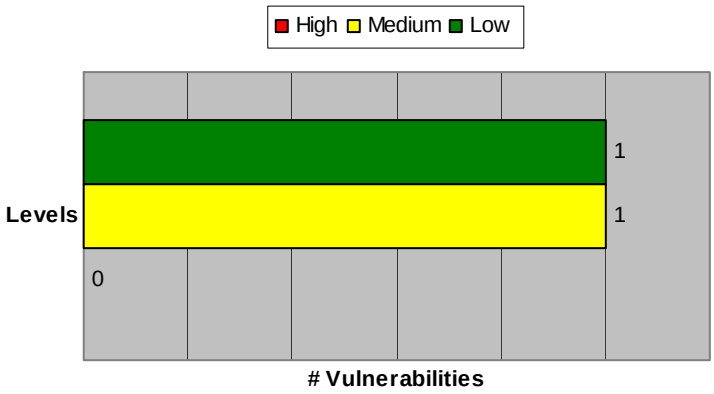


General Info		
OS fingerprint	Windows 2000	
Open TCP services	Number	Service
	80	HTTP
	443	HTTPS

- L'applicazione WEB presente su questo server presenta una maschera di Login. Il Cliente non ha fornito delle credenziali valide per un approfondito *Assessment Applicativo.* Cio' nonostante sono stati effettuati vari tentativi per aggirare il controllo di login (*SQL Injection, Parameter Tampering*, etc.) che **non** hanno prodotto risultati di rilievo.
- Le connessioni http vengono redirette su protocollo https.
- Analizzando gli header di risposta, il WebServer sembra essere Netscape-Enterprise/6.0

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
L2	Low	SSL Downgrade	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	Unito ad attacchi di traffic redirection (*route mangling, DNS poisoning,* etc.) potrebbe essere possibile impersonare il server verso altri client o decifrare il flusso di dati.	Se non utilizzati per ragioni di retrocompatibilita', disabilitare SSLv2 e l'utlizzo di chiavi minori di 128bit.

6.1.5 x.x.x.x.6 – www.XXXXxxxx.xxx

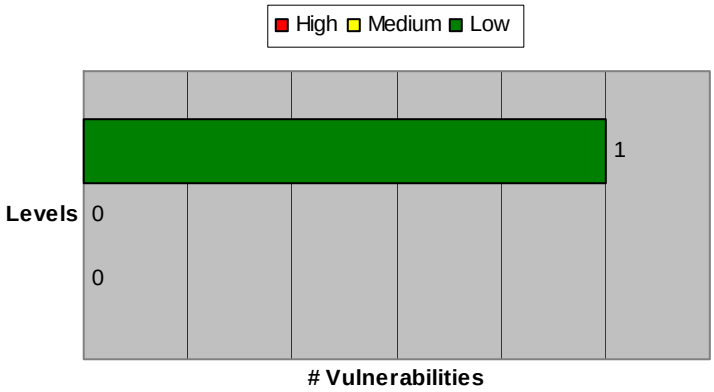


General Info		
OS fingerprint	Linux 2.4.x	
Open TCP services	Number	Service
	25	SMTP
	80	http

- La macchina offre un servizio SMTP per l'invio della posta elettronica. Il tentativo di utilizzarla come *Open Relay* **non** ha prodotto risultati di rilievo.
- La macchina ospita un WebServer (Apache) contenente le pagine del sito *www.XXXXxxxx.xxx*.
- Sul WebServer sono state trovate due directory di rilievo:
  - */admin/* - richiede autenticazione utente
  - */manual/* - contiene i manuali di utilizzo di Apache (consigliata l'eliminazione).

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
M1	Medium/High	PHP4 Multiple Vulnerabilities[3]	PHP4 contiene numerosi overflow all'interno di alcune funzioni come base64_encode() e ibase_blob_get()	E' possibile bloccare il servizio WEB o eseguire codice maligno sulla macchina.	Upgrade disponibile su http://www.php.net/downloads.php
L1	Low	Web Server Account Disclosure	Analizzando gli header in risposta a richieste per le home directory di utenti "standard", e' possibile risalire ad una lista di account validi.	Una lista di utenti validi puo' essere utilizzata da un intrusore nelle fasi avanzate di un attacco.	Disabilitare la direttiva "UserDir" nel file di configurazione httpd.conf: `UserDir Disabled`

6.1.6 x.x.x.x.7 – www1.xxxx.xxx



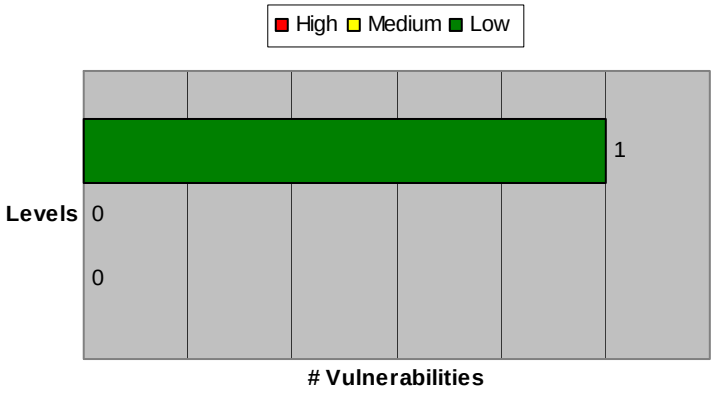
General Info		
OS fingerprint	Windows 2000	
Open TCP services	Number	Service
	443	HTTPS

[3] Nonostante la versione di PHP risulti vulnerabile, non e' stato trovato nessun *vettore di attacco* utile all'interno delle pagine php presenti sul server. Per essere sfruttata, la vulnerabilita' richiede infatti che una delle funzioni vulnerabili venga utilizzata su dei dati inseriti dall'utente. Non e' stato possibile verificare queste condizioni sulle pagine attualmente presenti sul server, e questo rappresenta un fattore mitigante.

- La pagina principale del sito web presenta un *redirect* verso https://www.xxxxXXXX.xx/home.html
- Analizzando gli header di risposta, il WebServer sembra essere Netscape-Enterprise/6.0

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
L2	Low	SSL Downgrade	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	Unito ad attacchi di traffic redirection (*route mangling, DNS poisoning,* etc.) potrebbe essere possibile impersonare il server verso altri client o decifrare il flusso di dati.	Se non utilizzati per ragioni di retrocompatibilita', disabilitare SSLv2 e l'utlizzo di chiavi minori di 128bit.

6.1.7 x.x.x.x.15 – www.xxxx.xx



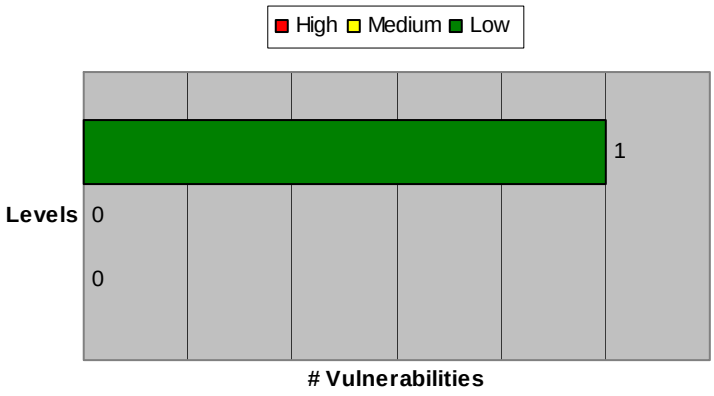
General Info		
OS fingerprint	Windows 2000	
Open TCP services	Number	Service
	443	HTTPS

- L'applicazione WEB presente su questo server presenta una maschera di Login. Il Cliente non ha fornito delle credenziali valide per un approfondito *Assessment Applicativo.* Cio' nonostante sono stati effettuati vari tentativi per aggirare il controllo di login (*SQL Injection, Parameter Tampering*, etc.) che **non** hanno prodotto risultati di rilievo.

- Analizzando gli header di risposta, il WebServer sembra essere Microsoft IIS 5.0

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
L2	Low	SSL Downgrade	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	Unito ad attacchi di traffic redirection (*route mangling, DNS poisoning,* etc.) potrebbe essere possibile impersonare il server verso altri client o decifrare il flusso di dati.	Se non utilizzati per ragioni di retrocompatibilita', disabilitare SSLv2 e l'utlizzo di chiavi minori di 128bit.

6.1.8 x.x.x.x.18 – xxxx.XXXX.xx

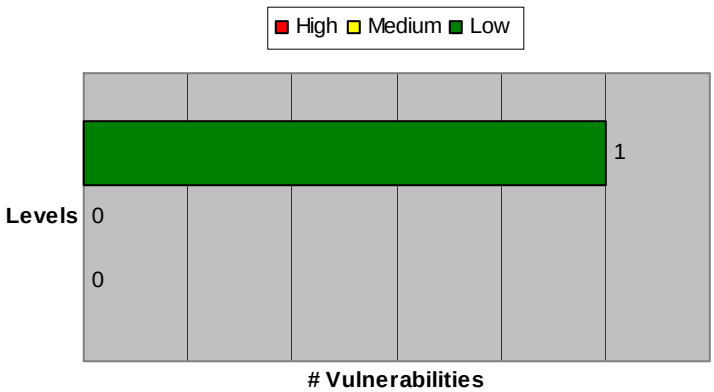


General Info		
OS fingerprint	Windows 2000	
Open TCP services	Number	Service
	443	HTTPS

- Analizzando gli header di risposta, il WebServer sembra essere Netscape-Enterprise/6.0

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
L2	Low	SSL Downgrade	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	Unito ad attacchi di traffic redirection (*route mangling, DNS poisoning,* etc.) potrebbe essere possibile impersonare il server verso altri client o decifrare il flusso di dati.	Se non utilizzati per ragioni di retrocompatibilita', disabilitare SSLv2 e l'utlizzo di chiavi minori di 128bit.
L3	Low	Physical Path Disclosure	Sul server sono installati dei *servlet* di default che rivelano l'alberatura fisica del file system.	Conoscere il path fisico dei file di sistema puo' agevolare un attacco nelle sue fasi avanzate.	Rimuovere i seguenti componenti: */server/HelloWorldServlet* */server/SimpleServlet* */server/SnoopServlet*

6.1.9 x.x.x.x.25 – www.xxxx-xxxx.xx

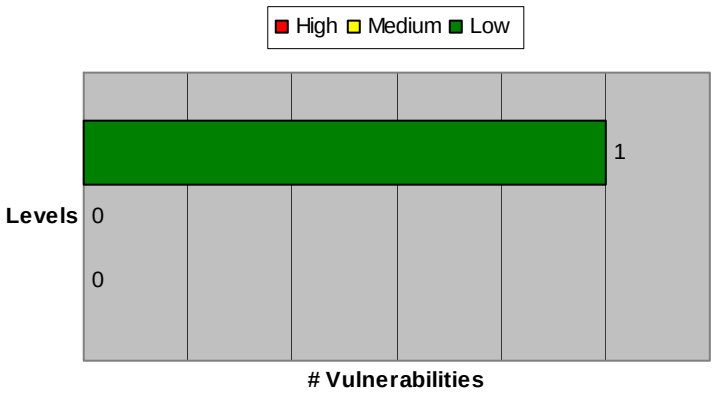


General Info		
OS fingerprint	Windows 2000	
Open TCP services	Number	Service
	443	HTTPS

- L'applicazione WEB presente su questo server presenta una maschera di Login. Il Cliente non ha fornito delle credenziali valide per un approfondito *Assessment Applicativo.* Cio' nonostante sono stati effettuati vari tentativi per aggirare il controllo di login (*SQL Injection, Parameter Tampering*, etc.) che **non** hanno prodotto risultati di rilievo.
- Analizzando gli header di risposta, il WebServer sembra essere Microsoft IIS 5.0

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
L2	Low	SSL Downgrade	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	Unito ad attacchi di traffic redirection (*route mangling, DNS poisoning,* etc.) potrebbe essere possibile impersonare il server verso altri client o decifrare il flusso di dati.	Se non utilizzati per ragioni di retrocompatibilita', disabilitare SSLv2 e l'utlizzo di chiavi minori di 128bit.

6.1.10 x.x.x.x.66 – (Nessun nome registrato)



General Info		
OS fingerprint	Solaris 7/8	
Open TCP services	Number	Service
	443	HTTPS

- L' FQDN presentato dal server nel suo certificato e' *xxx.XXXX.xx,* ma tale nome non sembra essere risolvibile dai DNS autoritativi per il dominio *XXXX.xx.*

- Accedendo al servizio HTTPS viene richiesta un autenticazione di tipo *Basic* con realm FW-1. Si puo' trattare di un *Authentication Proxy* o di un *SSL-VPN Gateway.*
- Analizzando i messaggi di errore di FW-1 e' possibile ipotizzare che il nome interno della macchina sia *xxxx*.
- Analizzando i messaggi di errore forniti in seguito al fallimento di un tentativo di login, e' possibile ipotizzare che esista l'utente *test.* Questo potrebbe facilitare tentativi di *BruteForcing* sulla password di accesso.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
L2	Low	SSL Downgrade[4]	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	Unito ad attacchi di traffic redirection (*route mangling, DNS poisoning,* etc.) potrebbe essere possibile impersonare il server verso altri client o decifrare il flusso di dati.	Se non utilizzati per ragioni di retrocompatibilita', disabilitare SSLv2, Anonymous Authentication e l'utlizzo di chiavi minori di 128bit.

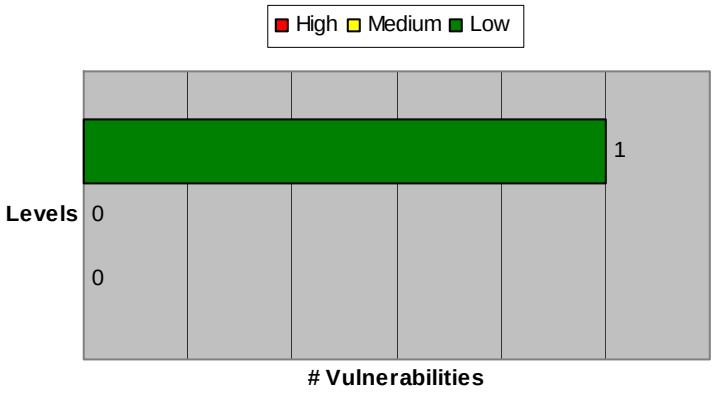
[4] In base al fingerprint del sistema operativo e delle applicazioni e' possibile ipotizzare che sia presente una versione di OpenSSL (0.9.6/7) vulnerabile a **ASN*.1 parsing vulnerability***. Su alcune piattaforme e' possibile generare un Denial Of Service (exploit pubblicamente disponibile) o addirittura esecuzione di codice maligno (exploit non disponibile). Non essendo stato possibile rilevare con precisione il tipo di software utilizzato, verificare il rilascio da parte del vendor di eventuali patch a tale vulnerabilita'

6.1.11 x.x.x.x.195 – (Nessun nome registrato)

General Info		
OS fingerprint	Solaris 7/8	
Open TCP services	Number	Service
	500	ISAKMP
Open UDP services	Number	Service
	500	ISAKMP

La macchina e' protetta da un dispositivo di packet-filtering e la sua funzione sembrerebbe essere quella di VPN-Gateway. Cio' nonostante, la macchina ha risposto negativamente ad ogni tentativo di negoziazione IKE.
Plausibilmente si puo' trattare di una vecchia versione di CheckPoint Firewall-1.

6.1.12 x.x.x.x.196 – (Nessun nome registrato)



General Info		
OS fingerprint	Solaris 7/8	
Open TCP services	Number	Service
	264	FW-1 SecuRemote
	443	HTTPS
	500	ISAKMP
Open UDP services	Number	Service
	500	ISAKMP

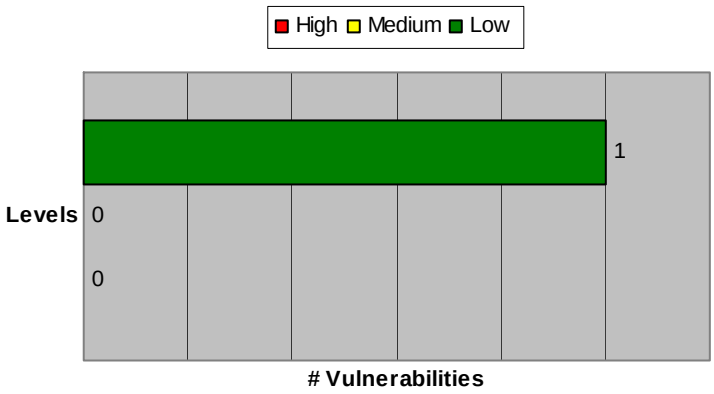
- L' FQDN presentato dal server nel suo certificato e' *xxx.XXXX.xx,* ma tale nome non sembra essere risolvibile dai DNS autoritativi per il dominio *XXXX.xx.*
- L'accesso al servizio HTTPS risulta bloccato da un dispositivo di filtraggio.
- Analizzando i messaggi di errore di FW-1 e' possibile ipotizzare che il nome interno della macchina sia *xxxx*.
- La macchina e' protetta da un dispostitivo di packet-filtering e la sua funzione sembrerebbe essere quella di VPN-Gateway. In seguito a uno scan delle policy, e' stato possibile risalire all'insieme di algoritmi crittografici e metodi di autenticazione supportati:

IKE Proposal			
Encryption Algorithm	Hash Algorithm	Group Description	Authentication
3DES-CBC	SHA	Alternate 1024bit MODP Group	RSA Signature
3DES-CBC	MD5	Alternate 1024bit MODP Group	RSA Signature
DES-CBC	SHA	Alternate 1024bit MODP Group	RSA Signature
DES-CBC	MD5	Alternate 1024bit MODP Group	RSA Signature

Il metodo di autenticazione basato su chiavi RSA **non** ha reso possibile alcun attacco di tipo *BruteForce* o *PasswordGuessing* per accedere alla VPN.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
L2	Low	SSL Downgrade	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	Unito ad attacchi di traffic redirection (*route mangling, DNS poisoning,* etc.) potrebbe essere possibile impersonare il server verso altri client o decifrare il flusso di dati.	Se non utilizzati per ragioni di retrocompatibilita', disabilitare SSLv2, Anonymous Authentication e l'utlizzo di chiavi minori di 128bit.

6.1.13 x.x.x.x.198 – (Nessun nome registrato)



General Info		
OS fingerprint	Solaris 7/8	
Open TCP services	Number	Service
	264	FW-1 SecuRemote
	443	HTTPS
	500	ISAKMP
Open UDP services	Number	Service
	500	ISAKMP

- L' FQDN presentato dal server nel suo certificato e' *xxxx.XXXX.xx,* ma tale nome non sembra essere risolvibile dai DNS autoritativi per il dominio *XXXX.xx.*
- L'accesso al servizio HTTPS risulta bloccato da un dispositivo di filtraggio.
- Analizzando i messaggi di errore di FW-1 e' possibile ipotizzare che il nome interno della macchina sia *xxxx*.
- La macchina e' protetta da un dispostitivo di packet-filtering e la sua funzione sembrerebbe essere quella di VPN-Gateway. In seguito a uno scan delle policy, e' stato possibile risalire all'insieme di algoritmi crittografici e metodi di autenticazione supportati:

IKE Proposal			
Encryption Algorithm	Hash Algorithm	Group Description	Authentication
3DES-CBC	SHA	Alternate 1024bit MODP Group	RSA Signature
3DES-CBC	MD5	Alternate 1024bit MODP Group	RSA Signature
DES-CBC	SHA	Alternate 1024bit MODP Group	RSA Signature
DES-CBC	MD5	Alternate 1024bit MODP Group	RSA Signature

Il metodo di autenticazione basato su chiavi RSA **non** ha reso possibile alcun attacco di tipo *BruteForce* o *PasswordGuessing* per accedere alla VPN.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
L2	Low	SSL Downgrade	Un attaccante nella posizione di *man-in-the-middle* puo' forzare l'utlizzo di protocolli di cifratura/autenticazione poco robusti.	Unito ad attacchi di traffic redirection (*route mangling, DNS poisoning,* etc.) potrebbe essere possibile impersonare il server verso altri client o decifrare il flusso di dati.	Se non utilizzati per ragioni di retrocompatibilita', disabilitare SSLv2, Anonymous Authentication e l'utlizzo di chiavi minori di 128bit.

6.1.14 x.x.x.x.199 – (Nessun nome registrato)

General Info		
OS fingerprint	Solaris 7/8	
Open TCP services	Number	Service
	264	FW-1 SecuRemote
	500	ISAKMP
Open UDP services	Number	Service
	500	ISAKMP

La macchina e' protetta da un dispostitivo di packet-filtering e la sua funzione sembrerebbe essere quella di VPN-Gateway. In seguito a uno scan delle policy, e' stato possibile risalire all'insieme di algoritmi crittografici e metodi di autenticazione supportati:

IKE Proposal			
Encryption Algorithm	Hash Algorithm	Group Description	Authentication
3DES-CBC	SHA	Alternate 1024bit MODP Group	RSA Signature

Il metodo di autenticazione basato su chiavi RSA **non** ha reso possibile alcun attacco di tipo *BruteForce* o *PasswordGuessing* per accedere alla VPN.

6.1.15 x.x.x.x.201 – (Nessun nome registrato)

General Info		
OS fingerprint	Solaris 7/8	
Open TCP services	Number	Service
	264	FW-1 SecuRemote
	500	ISAKMP
Open UDP services	Number	Service
	500	ISAKMP

La macchina e' protetta da un dispostitivo di packet-filtering e la sua funzione sembrerebbe essere quella di VPN-Gateway. In seguito a uno scan delle policy, e' stato possibile risalire all'insieme di algoritmi crittografici e metodi di autenticazione supportati:

IKE Proposal			
Encryption Algorithm	Hash Algorithm	Group Description	Authentication
3DES-CBC	SHA	Alternate 1024bit MODP Group	RSA Signature

Il metodo di autenticazione basato su chiavi RSA **non** ha reso possibile alcun attacco di tipo *BruteForce* o *PasswordGuessing* per accedere alla VPN.

6.1.16 x.x.x.x.252 – (Nessun nome registrato)

General Info		
OS fingerprint	Cisco IOS 11.3 - 12.3	
Open TCP services	Number	Service
	79	Finger
	514	Shell
Open UDP services	Number	Service
	123	ntp

Il servizio scelto per l'amministrazione remota della macchina (*rsa/rexec*) espone le credenziali dell'utente ad un attaccante in grado di monitorare il traffico. Se e' necessario amministrare da remoto la macchina, si consiglia di utilizzare il protocollo SSH.

6.1.17 x.x.x.x.253 – (Nessun nome registrato)

General Info		
OS fingerprint	Cisco IOS 11.3 - 12.3	
Open TCP services	Number	Service
	79	Finger
	514	Shell
Open UDP services	Number	Service
	123	ntp

Il servizio scelto per l'amministrazione remota della macchina (*rsa/rexec*) espone le credenziali dell'utente ad un attaccante in grado di monitorare il traffico. Se e' necessario amministrare da remoto la macchina, si consiglia di utilizzare il protocollo SSH.

6.1.18 x.x.x.106 – (Nessun nome registrato)[5]

General Info		
OS fingerprint	Nokia/CheckPoint	
Open TCP services	Number	Service
	264	FW-1 SecuRemote
	500	ISAKMP
Open UDP services	Number	Service
	500	ISAKMP

La macchina e' protetta da un dispostitivo di packet-filtering e la sua funzione sembrerebbe essere quella di VPN-Gateway. In seguito a uno scan delle policy, e' stato possibile risalire all'insieme di algoritmi crittografici e metodi di autenticazione supportati:

[5] x.x.x.106 e' l'unica delle machine esaminate a non trovarsi all'interno della rete x.x.x.0/22.
Tale macchina risulta essere raggiungibile tramite l'ISP xxxx.

IKE Proposal			
Encryption Algorithm	Hash Algorithm	Group Description	Authentication
3DES-CBC	SHA	Alternate 1024bit MODP Group	RSA Signature

Il metodo di autenticazione basato su chiavi RSA **non** ha reso possibile alcun attacco di tipo *BruteForce* o *PasswordGuessing* per accedere alla VPN.